D-Link

D-Link™ DGS-3100 Series
Gigabit Stackable Managed Switch

User Manual

V3.6

Information in this document is subject to change without notice.

© 2009 D-Link Computer Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Computer Corporation is strictly forbidden.

Trademarks used in this text: D-Link and the D-Link logo are trademarks of D-Link Computer Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Computer Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

VCCI Warning

この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

January, 2010 P/N

Table of Contents

PREFACE ..... **I**

System Overview ii
Viewing the Device iii
DGS-3100 Series Front Panel iii
DGS-3100-24TG Front Panel iii
Device Management Methods iv
User Guide Overview v
Intended Audience vi
Notes, Notices, and Cautions vii
Safety Cautions viii
General Precautions for Rack-Mountable Products ix

GETTING STARTED **1**

Accessing the Boot/Startup Menu Functions 2
Downloading Software 2
Set Terminal Baud-Rate 3
Defining Stacking Units 3
Using the Web-Based User Interface 5
Understanding the D-Link Embedded Web Interface 6
Using the Tool Menu 8
Displaying the Stack Status 8
Locating Devices 8
Backing up and Restoring Configuration Files 9
Resetting the Device 10
Downloading the Firmware 11
Rebooting the System 13
View/Add/Update/Delete User Accounts Using the Web System Components 14
'User' Level Support on the WEB 15

CONFIGURING BASIC CONFIGURATION **16**

Viewing Device Information 17
Defining System Information 19
Defining IP Addresses 20
Managing Stacking 21
Managing Stacking Modes 21
Advanced Stacking 21
Stack Startup Process 23
Building Stacks – Quick Start 25
Stack Management Examples 26
Configuring Stacking 32
Defining Ports 33
Configuring Port Properties 33
Viewing Port Properties 35
ARP Settings 36
Configuring User Accounts 37
Managing System Logs 39
Configuring SNTP 41
Configuring Daylight Savings Time 43

Configuring SNMP 47
Defining SNMP Settings 48
Defining SNMP Views 49
Defining SNMP Groups 50
Defining SNMP Users 52
Defining SNMP Communities 54
Defining SNMP Host Table 55
Defining SNMP Engine ID 57
Enabling SNMP Traps 58
DHCP Relay 59
DHCP Local Relay 60
DHCP Auto Configuration 62
Dual Image Services 63
Firmware Information 63
Config Firmware Image 64
Telnet Setting 65
Defining Time Ranges 66
Serial Port Settings 68
CONFIGURING L2 FEATURES 69
Enabling Jumbo Frames 70
Configuring VLANs 71
Understanding IEEE 802.1p Priority 71
VLAN Description 71
Notes about VLANs on the DGS-3100 Series 71
IEEE 802.1Q VLANs 71
802.1Q VLAN Tags 73
Port VLAN ID 74
Tagging and Untagging 74
Ingress Filtering 74
Default VLANs 75
VLAN and Trunk Groups 75
VLAN Status 75
Defining VLAN Properties 76
Defining Asymmetric VLAN 78
Configuring GVRP 80
Defining Trunking 82
Load Balancing 82
Defining VLAN Trunking 84
Traffic Segmentation 86
Configuring LACP 87
Defining IGMP Snooping 88
Defining MLD Snooping 91
Configuring Port Mirroring 95
Configuring Spanning Tree 97
Defining Spanning Tree Global Parameters 98
Defining STP Port Settings 100
Defining Multiple Spanning Tree Configuration Identification 102
Defining MSTP Port Information 103

Defining Forwarding and Filtering 105
Defining Unicast Forwarding 105
Defining Multicast Forwarding 106
Defining Multicast Filtering 107
Defining DLF Filtering 108
Configuring LLDP 110
Defining LLDP Global Settings 110
Defining LLDP Port Settings 111
Defining LLDP Basic TLV Settings 113
Defining LLDP Dot3 TLV Settings 114
Viewing LLDP Local Port Information 115
Viewing LLDP Remote Port Information 117
Configuring Voice VLAN 122
Defining Voice VLAN Port Settings 123
Defining OUIs 124
CONFIGURING QUALITY OF SERVICE 126
Understanding QoS 128
Defining Bandwidth Settings 129
Configuring Storm Control 131
Mapping Ports to Packet Priorities 133
Mapping Priority to Classes (Queues) 134
Configuring QoS Scheduling Mechanism 135
Defining DSCP User Priority 136
Defining Multi-Layer CoS Settings 137
SECURITY FEATURES 138
Configuring Safeguard Engine 139
Configuring Trust Host 140
Configuring Port Security 142
Configuring Guest VLANs 144
Configuring Port Authentication 802.1X 145
Configuring MAC Authentication (by using Guest VLAN, 802.1X and Radius pages) 150
Defining RADIUS Settings 153
Defining EAP Forwarding Settings 155
Configuring Secure Socket Layer Security 156
Configuring Secure Shell Security 158
Defining SSH Algorithm Settings 159
Defining Application Authentication Settings 161
Configuring Authentication Server Hosts 163
Defining Login Methods 164
Defining Enable Methods 166
Configuring Local Enable Password 168
Defining ARP Spoofing Prevention Settings 169
MONITORING THE DEVICE 171
Viewing Stacking Information 172
Viewing CPU Utilization 173
Viewing Port Utilization 174
Viewing Packet Size Information 175

Viewing Received Packet Statistics 176
Viewing UMB_cast Packet Statistics 177
Viewing Transmitted Packet Statistics 178
Viewing RADIUS Authenticated Session Statistics 180
Viewing ARP Table 181
Viewing MLD Router Ports 182
Viewing Router Ports 183
Viewing Session Table 184
Viewing IGMP Group Information 185
Viewing MLD Group Information 186
Defining Dynamic and Static MAC Addresses 187
Viewing System Log 189
Green Ethernet 190
Device Environment 191
Errors 192
Cable Diagnostics 195
MANAGING POWER OVER ETHERNET DEVICES 197
Defining PoE Port Information 198
Configuring PoE System Settings 200
DEFINING ACCESS PROFILE LISTS 201
Methods for Defining Access Control Lists 202
ACL Configuration Wizard 203
Defining Access Profile Lists 205
Defining Layer 3 IPv6 ACL 218
IP and MAC-Based ACLs on the Same Port 224
Adding Access Rules 224
Finding ACL Rules 228
CONNECTORS AND CABLES 232
Pin Connections for the 10/100/1000 Ethernet Interface 233
RJ-45 Ports Pinout 233
Pin Connections for the HDMI Connector 234
HDMI Ports Pinout 234
SYSLOG ERRORS 235
PASSWORD RECOVERY PROCEDURE 279

Preface

This preface provides an overview to the guide, and includes the following sections:

- System Overview
- Viewing the Device
- Device Management Methods
- User Guide Overview
- Intended Audience
- Notes, Notices, and Cautions
- Safety Cautions
- General Precautions for Rack-Mountable Products

System Overview

The DGS-3100 series and the DGS-3100-24TG Gigabit Ethernet Switches enhance networks by providing a powerful switch that eliminates network bottlenecks, enabling network administrators to fine tune network configurations.

The DGS-3100 series and the DGS-3100-24TG are perfect for departmental and enterprise connections, and are ideal for backbone and server connections.

Viewing the Device

The devices described in this section are stackable Gigabit Ethernet Managed Switches. Device management is performed using an Embedded Web Server (EWS) or through a Command Line Interface (CLI). The device configuration is performed via an RS-232 interface. This section contains descriptions for the following:

- DGS-3100 series Front Panel
- DGS-3100-24TG Front Panel

DGS-3100 Series Front Panel

The DGS-3100 series provides 24/48 high performance 1000BASE-T ports. The 1000Base-T ports operate at 10/100/1000, and connect to backbones, end-stations, and servers. The DGS-3100 series also provides 4 Mini-GBIC (SFP) combo ports which connect fiber optic media to switches, servers, or network backbone. The DGS-3100 series provides an additional RS-232 port (console port) for managing the switch via a console terminal or PC with a Terminal Emulation Program.

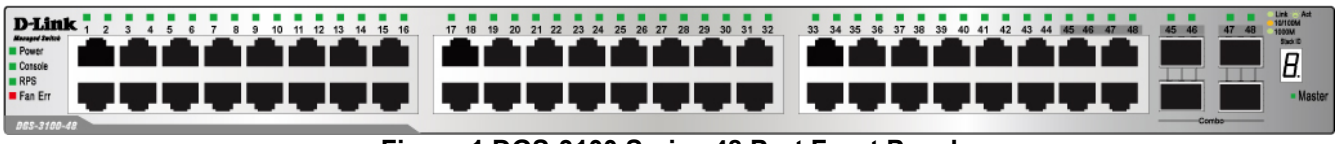


Figure 1 DGS-3100 Series 48 Port Front Panel

DGS-3100-24TG Front Panel

The DGS-3100-24TG provides eight high performance 1000BASE-TX ports. The ports operate at 10/100/1000, and connect to backbones, end-stations, and servers. The DGS-3100-24TG also provides 16 Mini-GBIC (SFP) ports which connect fiber optic media to switches, servers, or network backbone. The DGS-3100-24TG provides an additional RS-232 port (console port) for managing the switch via a console terminal or PC with a Terminal Emulation Program.

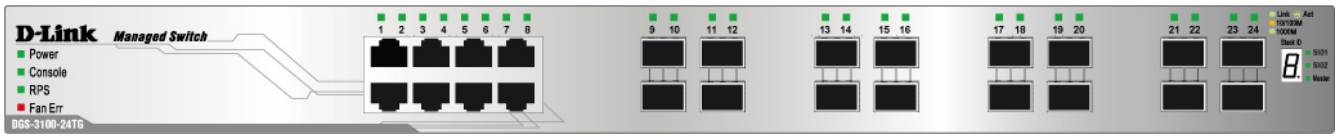


Figure 2 DGS-3100-24TG Front Panel

Device Management Methods

The DGS-3100 series and DGS-3100-24TG provide different methods for managing the device including:

- Web Based Management Interface
- SNMP-Based Management
- Command Line Console

Web Based Management Interface

Once the device is installed, network managers can configure the switch, monitor the LED panel, and display statistics graphically via a web browser, including:

- Netscape Navigator (version 7.0 and higher)
- Microsoft® Internet Explorer (version 5.0 and higher)
- Mozilla Firefox (version 2.0 and higher)
- Apple Safari

SNMP-Based Management

The system also supports SNMPv1, SNMPv2c, and SNMPv3. The SNMP agent decodes the incoming SNMP messages, and replies to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Command Line Console

The device also supports device configuration using the *Command Line Interface*. A terminal is connected to device via the serial console port.

User Guide Overview

This section provides an overview to the DGS-3100 series and the DGS-3100-24TG Switch Manual, including the guide structure and a chapter overview:

- **Section 1, Getting Started** — Provides general background for understanding and using the Boot/Startup Menu and the Embedded Web System, including an explanation of the interface buttons and general system functions.
- **Section 2, Defining the Basic Device Configuration** — Provides information for viewing system information, defining IP addresses, managing stacking, defining ports, configuring SNMP management, and defining the system time settings.
- **Section 3, Configuring L2 Features** — Provides information for enabling and configuring Jumbo frames, VLANs, Trunks (LAGs), Traffic Segmentation, Multicast forwarding, Spanning Tree and LLDP.
- **Section 4, Configuring Quality of Service** — Provides information for ability to implement QoS and priority queuing within a network.
- **Section 5, Security Features** — Provides information for enabling and configuring device security.
- **Section 6, Monitoring the Device** — Provides information for monitoring the device.
- **Section 7, Managing Power over Ethernet Devices** — Provides information configuring the PoE function.
- **Section 8, Defining Access Profile Lists** — Provides information for configuring the ACL.

Intended Audience

The DGS-3100 series/DGS-3100-24TG User Guide contains information for configuring and managing the DGS-3100 series/DGS-3100-24TG Switches. This guide is intended for network managers familiar with network management concepts and terminology.

Notes, Notices, and Cautions

NOTE: A NOTE indicates important information that helps you make better use of your device.

NOTICE: A NOTICE indicates ***either*** potential damage to hardware or loss of data and tells you how to avoid the problem.

CAUTION: A CAUTION indicates a potential for property damage, personal injury, or death.

Safety Cautions

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage. Throughout this safety section, the caution icon ( ) is used to indicate cautions and precautions that you need to review and follow.

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the following precautions.

- Do not service any product except as explained in your system documentation. Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock. Only a trained service technician should service components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
  - The power cable, extension cable, or plug is damaged.
  - An object has fallen into the product.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block the cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause a fire or an electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- To help avoid damaging your system, be sure the voltage selection Switch (if provided) on the power supply is set to match the power available at your location:
  - 115 volts (V)/60 hertz (Hz) in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
  - 100 V/50 Hz in eastern Japan and 100 V/60 Hz in western Japan
  - 230 V/50 Hz in most of Europe, the Middle East, and the Far East
- Also be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent an electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.

- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
  - Install the power supply before connecting the power cable to the power supply.
  - Unplug the power cable before removing the power supply.
  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.

Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

General Precautions for Rack-Mountable Products

Observe the following precautions for rack stability and safety. Also refer to the rack installation documentation accompanying the system and the rack for specific caution statements and procedures.

Systems are considered to be components in a rack. Thus, "component" refers to any system as well as to various peripherals or supporting hardware.

CAUTION: Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack.

After installing system/components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.

Always load the rack from the bottom up, and load the heaviest item in the rack first.

Make sure that the rack is level and stable before extending a component from the rack.

Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.

After a component is inserted into the rack, carefully extend the rail into a locking position, and then slide the component into the rack.

Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.

Ensure that proper airflow is provided to components in the rack.

Do not step on or stand on any component when servicing other components in a rack.

NOTE: A qualified electrician must perform all connections to DC power and to safety grounds. All electrical wiring must comply with applicable local or national codes and practices.

CAUTION: Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

CAUTION: The system chassis must be positively grounded to the rack cabinet frame. Do not attempt to connect power to the system until grounding cables are connected. Completed power and safety ground wiring must be inspected by a qualified electrical inspector. An energy hazard will exist if the safety ground cable is omitted or disconnected.

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your system. To prevent static damage, discharge static electricity from your body before you touch any of the electronic components, such as the microprocessor. You can do so by periodically touching an unpainted metal surface on the chassis.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

1. **When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.**
2. **When transporting a sensitive component, first place it in an antistatic container or packaging.**
3. **Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads and an antistatic grounding strap.**

Battery Handling Reminder

CAUTION: This is danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

1

GETTING STARTED

To begin managing the device, simply run the browser installed on the management station and point it to the IP address defined for the device. For example; http:///123.123.123.123. Please note that the proxy for session connection should be turned off.

NOTE: The Factory default IP address for the Switch is 10.90.90.90.

Accessing the Boot/Startup Menu Functions

The following configuration functions are performed from the Boot (Startup) menu:

- Downloading Software
- Set Terminal Baud-Rate
- Defining Stacking Units

To display the Startup menu:

1. During the boot process, after the first part of the POST is completed press Ctrl+shift+ (-) within 2 seconds after the following message is displayed**:**

Autoboot in 2 seconds –press RETURN or Esc. to abort and enter prom.#

2. Press Enter to access the Startup menu.
3. The Startup menu is displayed and contains the following configuration functions**.**

Startup Menu
[1] Download Software
[2] Set Terminal Baud-Rate
[3] Stack menu
[4] Back
Enter your choice or press 'ESC' to exit:

The following sections describe the Startup menu options. If no selection is made within 25 seconds (default), the switch times out and the device continues to load normally.

Downloading Software

Use the software download option when a new software version must be downloaded to replace corrupted files, update, or upgrade the system software. It is recommended to set the Baud Rate to 38400 prior to downloading software, therefore allowing the software download to be faster. See *Set Terminal Baud-Rate*.

To download software from the Startup menu:

1. On the Startup menu, press "1".

The following prompt is displayed:

Downloading code using XMODEM

2. When using HyperTerminal, click Transfer on the HyperTerminal menu bar.
3. From the Transfer menu, click Send File. The Send File window is displayed.
4. Enter the file path for the file to be downloaded.
5. Ensure the protocol is defined as Xmodem.
6. Click Send**.**

The software is downloaded. Software downloading takes several minutes. The terminal emulation application, such as HyperTerminal, may display the progress of the loading process. After software downloads, the device reboots automatically. Refer to the *Set Terminal Baud-Rate* section to define the Terminal Baud-Rate.

NOTE**:** Previous firmware versions that do not support Green Ethernet and Fan Control cannot be downloaded into boards with Hardware version B1. The download fails after the device recognizes a firmware version that does not support these features.

Set Terminal Baud-Rate

Use the Set Terminal Baud-Rate option to define the Baud-Rate. The Baud-Rate is the serial bit rate used to communicate with the management host. The Baud-Rates values are: 2400, 4800, 9600, 19200, 38400. The default Baud-Rate value is 9600.

To set the terminal Baud-Rate:

1. **On the Startup menu, press "2".**

The following prompt is displayed:

Set new device Baud rate: _

2. **Press Enter to apply changes.**

Defining Stacking Units

Use the Stack menu option to display the current stack unit ID list and define an alternative unit ID (stack membership number). Unit ID 0 is allocated for auto-numbering, which is the factory default. Refer to *Managing Stacking* for further reference.

To access the stack menu:

1. **On the Startup menu, press "3".**

The following prompt is displayed:

Stack menu

[1] Show unit stack id
[2] Set unit stack id
[3] Back
Enter your choice or press 'ESC' to exit:

2. **To display the current unit stack ID list, press "1".**

The following prompt is displayed:

Stack menu

[1] Show unit stack id
[2] Set unit stack id
[3] Back
Enter your choice or press 'ESC' to exit:

Current working mode is stacking.
Unit stack id set to 0.

===== Press Enter to Continue ====

3. **To change the unit ID (stack membership number), press "2".**

The following prompt is displayed:

Stack menu

[1] Show unit stack id
[2] Set unit stack id
[3] Back
Enter your choice or press 'ESC' to exit:

Enter unit stack id [0-6]:

Using the Web-Based User Interface

This section contains information on starting the D-Link Embedded Web Interface. To access the D-Link user interface:

1. Open an Internet browser. Ensure that pop-up blockers are disabled. If pop-up blockers are enabled, edit, add, and device information messages may not open.
2. Enter the device IP address in the address bar and press *Enter*.

The user interface provides access to various switch configuration and management windows, allows you to view performance statistics, and permits you to graphically monitor the system status. The screen captures in this Guide represent the DGS-3100-48 48 port device. The Web pages in the 24 port and the DGS-3100-24TG devices may vary slightly.

Understanding the D-Link Embedded Web Interface

The D-Link Embedded Web Interface Device Information Page contains the following information:

View	Description
Tree View	Displays the different system features, and configuration options.
Zoom View	Located at the top of the home page, the port LED indicators provide a visual representation of the ports on the D-Link front panel.
Menu Information View	Located below the Zoom View, displays *Save*, *Tool* menu, *Stack ID*, and *Logout* buttons. Also displays Up Time information and User Loggin Identification.
Device Information View	Located in the main part of the home page, the device view provides a view of the device, an information or table area, and configuration instructions.
Stacking Status View	Located at the bottom left corner of the home page, the stacking status view provides a graphic representation of the stacking links and ports status.

Table 0-1 Web Interface Views

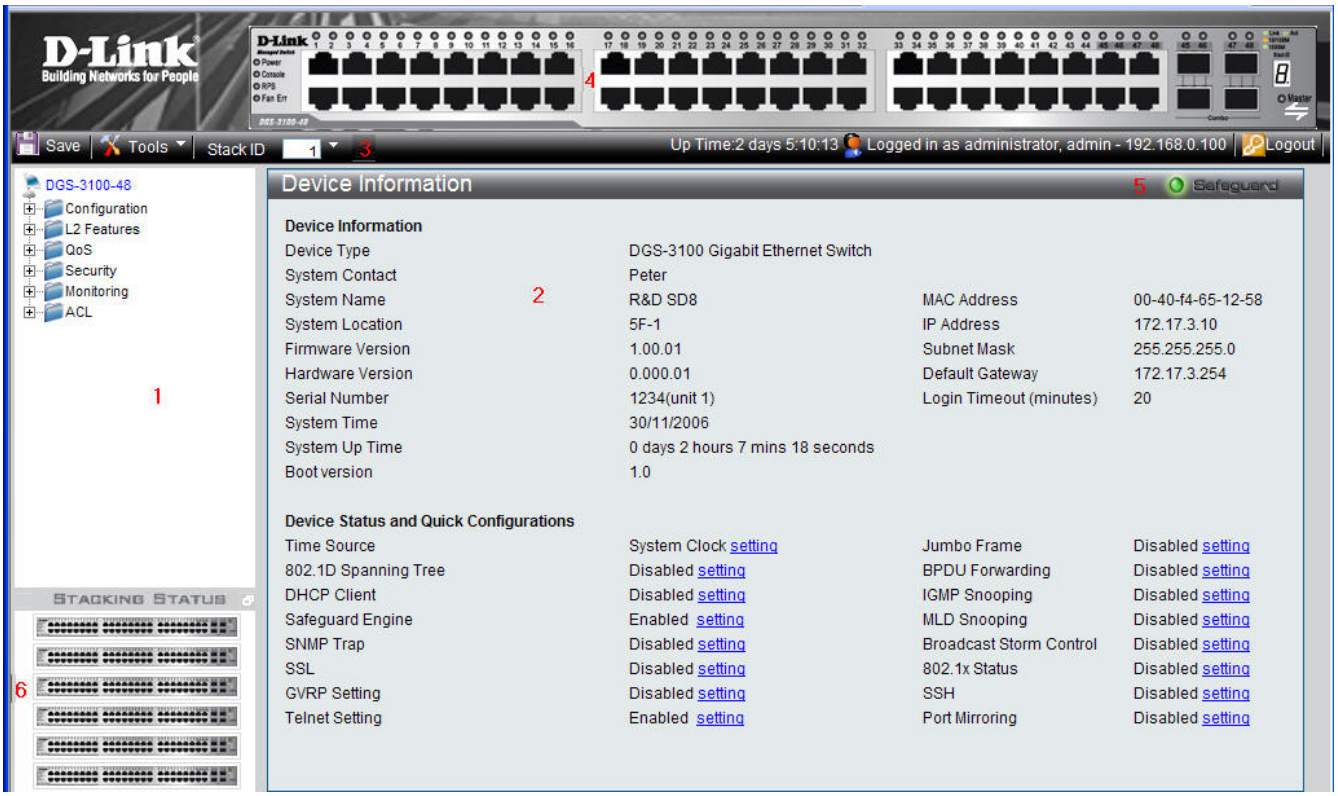


Figure 0-1 Device Information Page

The following table describes the main 6 areas on the Device Information Page:

View	Description
1. Tree View	Select the folder or window to be displayed. The folder icons can be opened to display the hyperlinked menu buttons and subfolders contained within them.
2. Device Information View	Presents Switch information based on the selection and the entry of configuration data
3. Menu Information View	Presents the *Save* button, a menu for accessing device tools, and a menu for Stack ID selection. The current Up Time and current User Loggin information is reported. The *Logout* button is also here.
4. Zoom View	Presents a graphical near real-time image of the front panel of the Switch. This area displays

View	Description
	the Switch's ports and expansion modules, showing port activity, duplex mode, or flow control, depending on the specified mode. Various areas of the graphic can be selected for performing management functions, including port configuration
5 Device Application Buttons	Provides access to the device logout, and provides information about the Safe Guard mode currently enabled on the device.
6 Stacking Status View	Provides a graphic representation of the stacking links and ports status.

Table 0-2 Main Areas

Using the Tool Menu

The tool menu contains menu options for:

- Displaying the Stack Status
- Locating Devices
- Backing up and Restoring Configuration Files
- Resetting the Device
- Downloading the Firmware
- Rebooting the System

Displaying the Stack Status

The *Stacking Information Page* provides specific information for stacked devices. For more information regarding the stacking setup, see Managing Stacking section.

Locating Devices

The *Device Locator Page* enables locating system devices by activating LED locators. To locate devices:

1. Click Tools > **Device Locator**. The *Device Locator Page* opens**.**

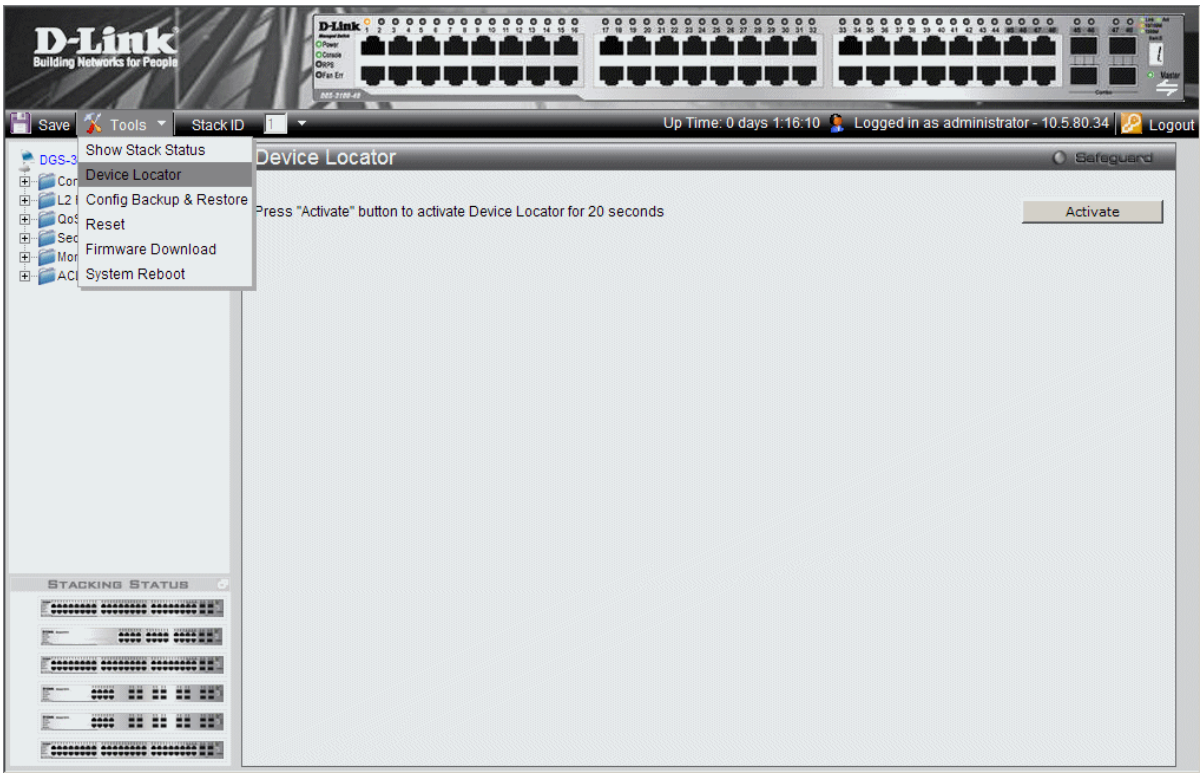


Figure 0-2 Device Locator Page

2. Click Activate. The LED locator is activated for 20 seconds On which the letter “L” will flash on the master unit.

Backing up and Restoring Configuration Files

The *Config Backup and Restore Page* contains fields for downloading and uploading the configuration file from the device through HTTP or TFTP server. To back up and restore configuration files:

1. Click Tools > **Config Backup & Restore**. The *Config Backup and Restore Page* opens.

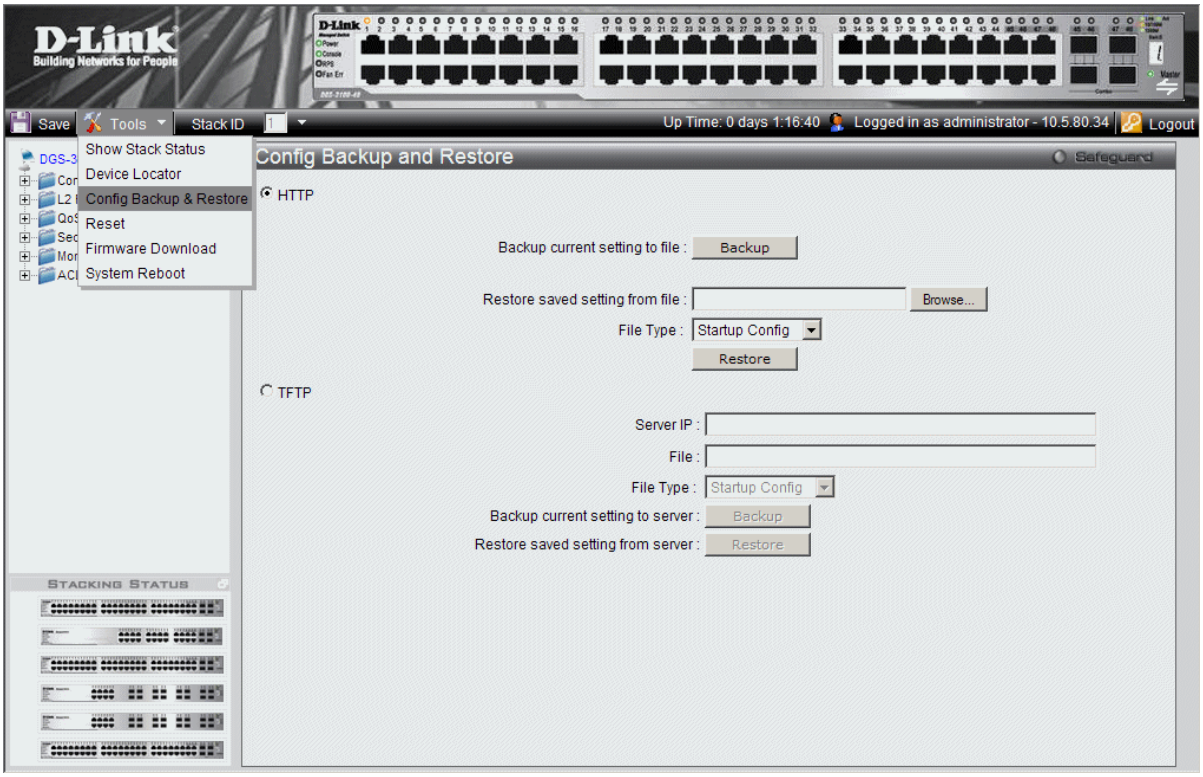


Figure 0-3 Config Backup and Restore Page

The Config Backup and Restore Page contain the following fields:

Field	Description
Http	Indicates that the system files are backed up or restored via an HTTP server. The possible field values are: *Backup current setting to file* — Backs up the current configuration files via the HTTP server. *Restore saved setting from file* — Restores the current configuration files via the HTTP server. *File Type* — Specifies the current configuration file type. The possible field values are *Startup Config* and *Running Config*.
TFTP	Indicates that the system files are backed up or restored via an TFTP server. The possible field values are: *Server IP* — Specifies the TFTP Server IP Address to which files are backed up or from which they are restored. *File* — Indicates the file that is backed up or restored. *File Type* — Specifies the current configuration file type. The possible field values are *Startup Config* and *Running Config*. *Backup current setting to server* — Backs up the current configuration files via the TFTP server. *Restore saved setting from server* — Restores the current configuration files via the TFTP server.

2. Select *HTTP* or *TFTP* field.
3. Define the selected server method fields.

To backup files, click Backup.

To restore files, click Restore.

Resetting the Device

The *Factory Reset Page* restores the factory defaults. To restore the device to the factory default settings:

1. Click Tools > **Reset**. The *Factory Reset Page* opens**:**

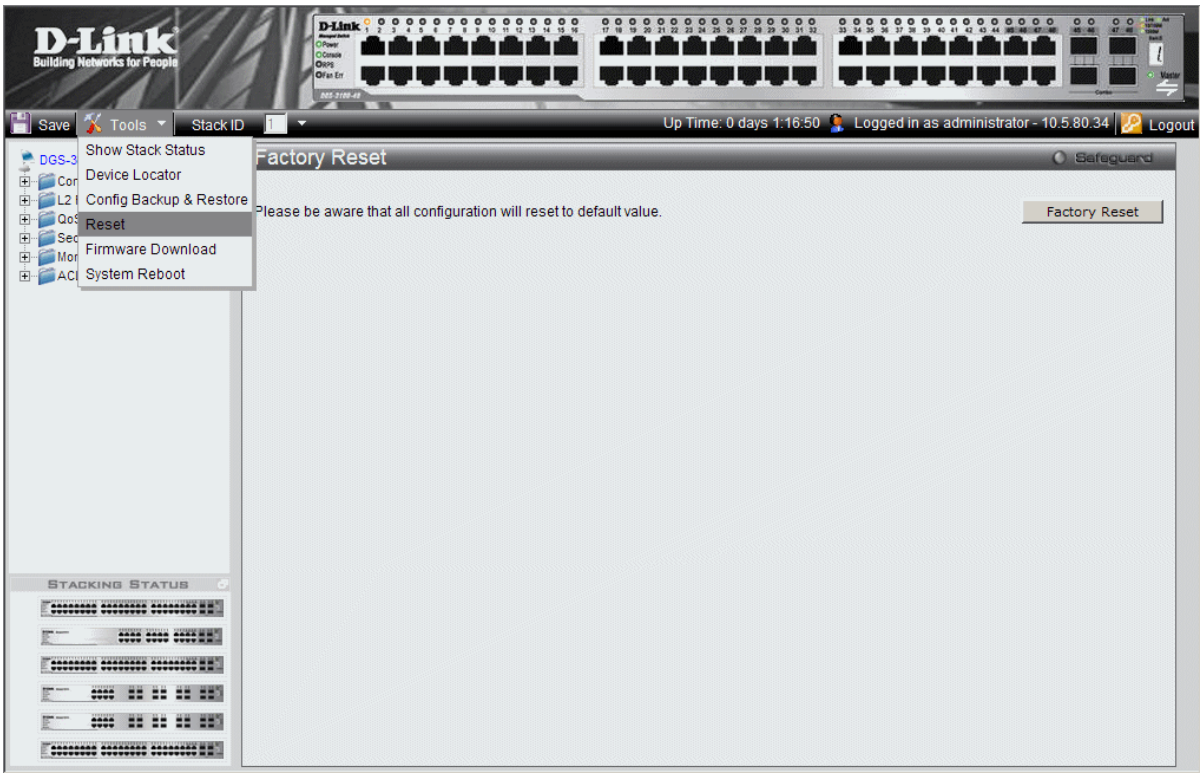


Figure 0-4 Factory Reset Page

2. Click Factory Reset. The factory default settings are restored once it completely reloaded, and the device is updated**.**

Downloading the Firmware

The 'Firmware Download' web page is used to download the firmware files that will be used to manage the device.

NOTE: Firmware version 1.x.x supports 4 SKUs od DGS-3100 series: DGS-3100-24, DGS-3100-24P, DGS-3100-48 and DGS-3100-48P, Firmware version 2.x.x supports in addition the 5th SKU: DGS-3100-24TG.

Firmware version 2.x.x includes as well additional features comparing to version 1.x.x, for more details, please refer to the Release Notes.

When upgrading firmware from version 1.x.x to version 2.x.x on the switch, the user should upgrade the boot software as well from version 1.0.0.3 to version 1.0.0.4.

Previous firmware versions that do not support Green Ethernet and Fan Control cannot be downloaded into boards with Fan Control and Green Ethernet. The download fails after the device recognizes a firmware version that does not support these features.

Upgrade Procedure – Important Notes:

ACL backward compatibility issue - In firmware 1.x.x, TCP/UDP ports of access profile are in hexadecimal instead of decimal values. In version 2.x.x, TCP/UDP port value entries are in decimal value. However - if the user upgrades the switch firmware from version 1.x.x to version 2.x.x, the value will be retained as hexadecimal value.

ACLs access rules priority did not work in firmware version 1.x.x. In firmware version 2.x.x, the priority is supported and it is not allowed two identical access rules priority from different access profiles. If the user download configuration file from version 1.x.x which including ACLs which has more than one rule, it might not work and there will be an error message. The user can delete and create the ACLs again if he encountered a problem.

Tacacs/Radius backwards compatibility issue - In firmware version 1.x.x, it is possible to configure up to 4 Tacacs /Radius servers. In firmware version 2.x.x, it is possible to configure up to 3 servers from each type. In addition to that it was not required to configure priority to Tacacs servers in 1.x.x while in 2.x.x it is required. If the user configured 4 servers in version 1.x.x and try to download the configuration to firmware 2.x.x, he will get an error message, the same event will happened because of the Tacacs priority.

The *Firmware Download Page* enables downloading files either via an HTTP or a TFTP server. To download Firmware:

1. Click Tools > **Firmware Download**. The *Firmware Download Page* opens**:**

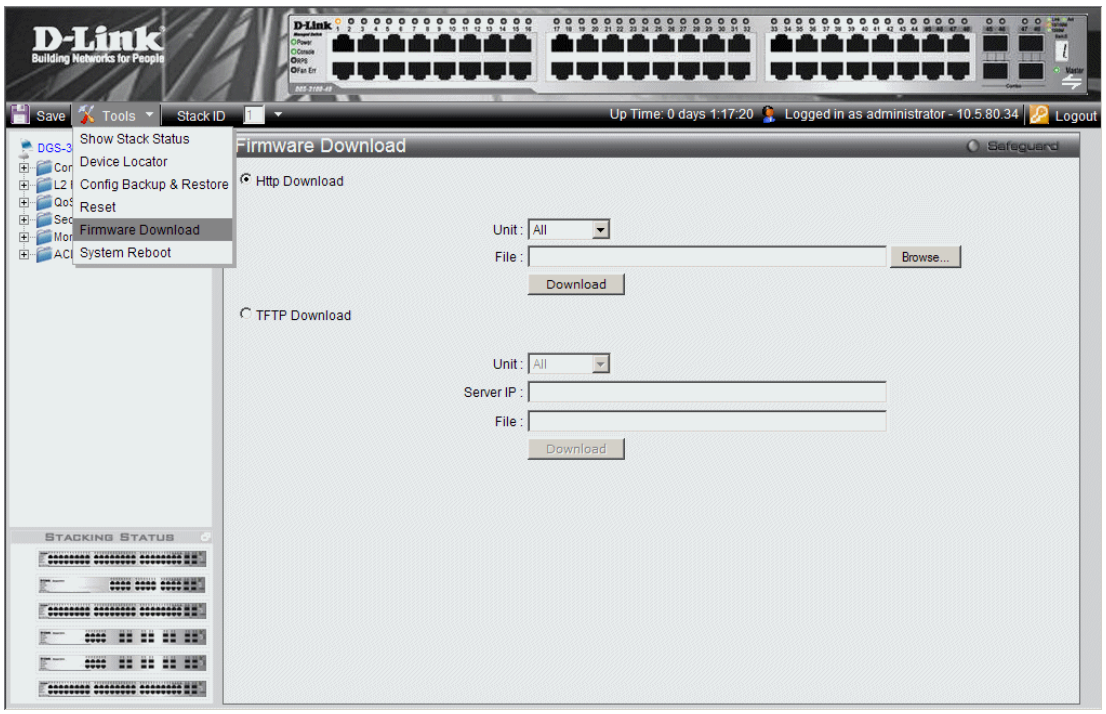


Figure 0-5 Firmware Download Page

The Firmware Download Page contains the following fields:

Field	Description
HTTP Download	Indicates that the Firmware file is downloaded via an HTTP server. *Unit* — Indicates if the Firmware file is downloaded to a specific stacking member or to All stacking members. *File* — Indicates the Firmware file that is downloaded to the stack or specific device.
TFTP Download	Indicates that the Firmware file is downloaded via a TFTP server. *Unit* — Indicates if the Firmware file is downloaded to a specific stacking member or to All stacking members. *Server IP Address* — Specifies the TFTP Server IP Address from which files are downloaded. *File* — Indicates the Firmware file that is downloaded to the stack or specific device.

2. Select *HTTP* or *TFTP* Download field.
3. Define the *Unit* field.
4. For *Http* download, define the *File* field, or alternatively, browse to select the file.
5. Click Download. The Firmware is downloaded, and the device is updated.

Rebooting the System

The *System Reboot Page* provides a method for selecting one, or all of the units to be rebooted. To reboot the system:

1. Click Tools > **System Reboot.** The *System Reboot Page* opens:

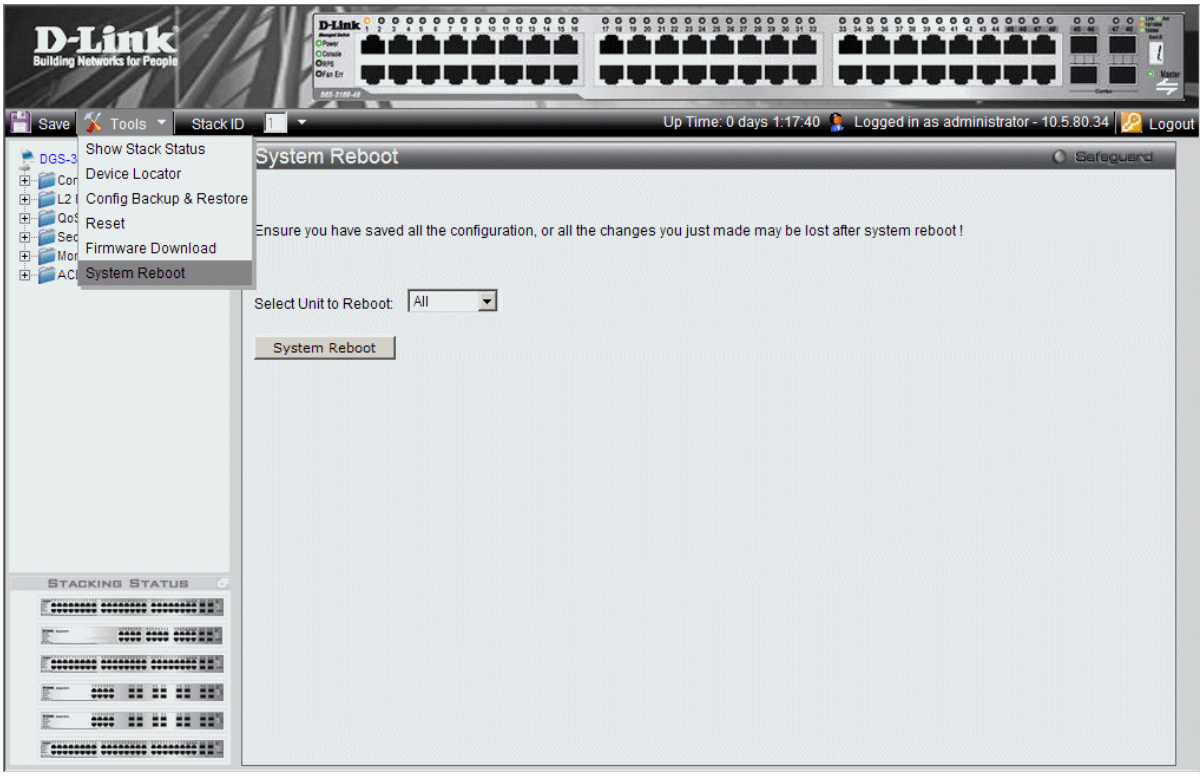


Figure 0-6 System Reboot Page

The System Reboot Page contains the Select Unit to Reboot field. The possible values are:

Value	Description
All	Reboots all stacking members.
01 - 06	Reboots the specific stack member.

2. Define the Select Unit to Reboot field.
3. Click System Reboot. The selected unit(s) is/are rebooted.

View/Add/Update/Delete User Accounts Using the Web System Components

The following table contains information regarding the list of buttons:

Component	Name	Description
Activate	Activate	Activates field commands
Add	Add	Adds selected items
All	ALL	Selects all
Apply	Apply	Applies field settings
Backup	Backup	Evokes backup
Cancel	Cancel	Cancels settings
Clear	Clear	Clears selected settings and fields
Clear All Entry	Clear All	Clears all settings and fields
Delete	Delete	Deletes selected fields
Delete VID	Delete VID	Deletes VLAN Identification
Download	Download	Starts downloading system files.
Edit	Edit	Modifies configuration Information
Factory Reset	Factory Reset	Resets the factory defaults
Find	Find	Finds a table entry.
System Reboot	System Reboot	Reboot the system
Refresh	Refresh	Refreshes device information.
Restore	Restore	Restores the specific configuration file.
View All Entry	View All Entry	Displays table entries.

Table 1-3 User Interface Buttons

'User' Level Support on the WEB

P3.0 firmware release will support additional user level (in addition to "Operator" and "Admin") on the WEB GUI. The new level will be ‘User’ (level 1).

‘User’ will have access as reader without possibility to change configuration to most of the web pages, except the pages that controls the following functionality that will be blocked to ‘user’ level:

- Update Firmware
- Modify/Delete startup configuration
- Factory Reset
- View/Add/Update/Delete User Accounts

If the 'User' is trying to modify any configuration by pressing the 'Apply' button, the ‘Access Denied’ page will be displayed.

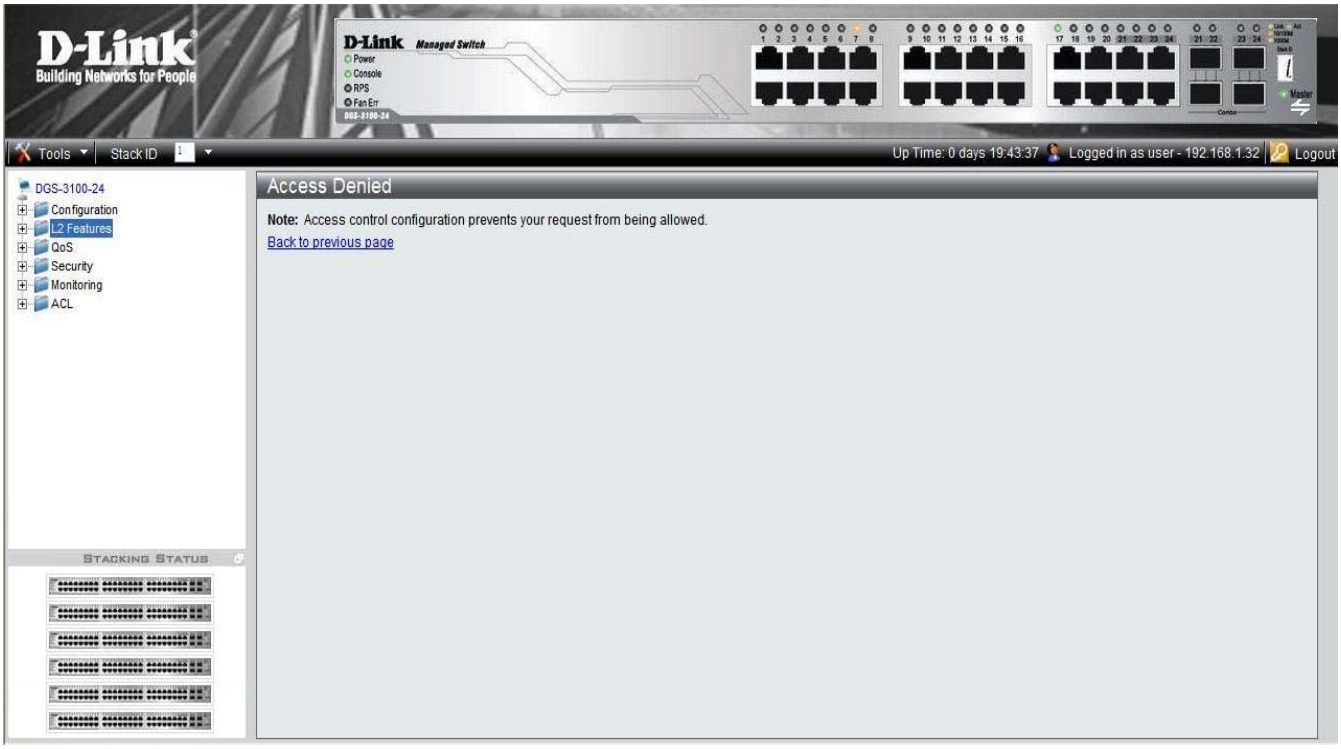


Figure 0-7 Access Denied Page

2

CONFIGURING BASIC CONFIGURATION

This section contains information for viewing device information, defining IP addresses, managing stacking, defining port parameters, configuring system user accounts, configuring and managing system logs, defining the system time, and configuring SNMP system management. This section contains the following topics:

- Viewing Device Information
- Defining System Information
- Defining IP Addresses
- Managing Stacking
- Defining Ports
- ARP Settings
- Configuring User Accounts
- Managing System Logs
- Configuring SNTP
- Configuring SNMP
- DHCP Relay
- DHCP Local Relay
- DHCP Auto Configuration
- Dual Image Services
- Telnet Setting
- Defining Time Ranges
- Serial Port Settings

Viewing Device Information

The *Device Information* Page contains parameters for configuring general device information, including the system name, location, and contact, the system MAC Address, System Up Time, and MAC addresses, and both software, boot, and hardware versions.

In addition the *Device Information* Page provides shortcuts to device feature pages. To define the general system information:

- Click **DGS-3100-xx** in the Tree View. The *Device Information* Page opens:

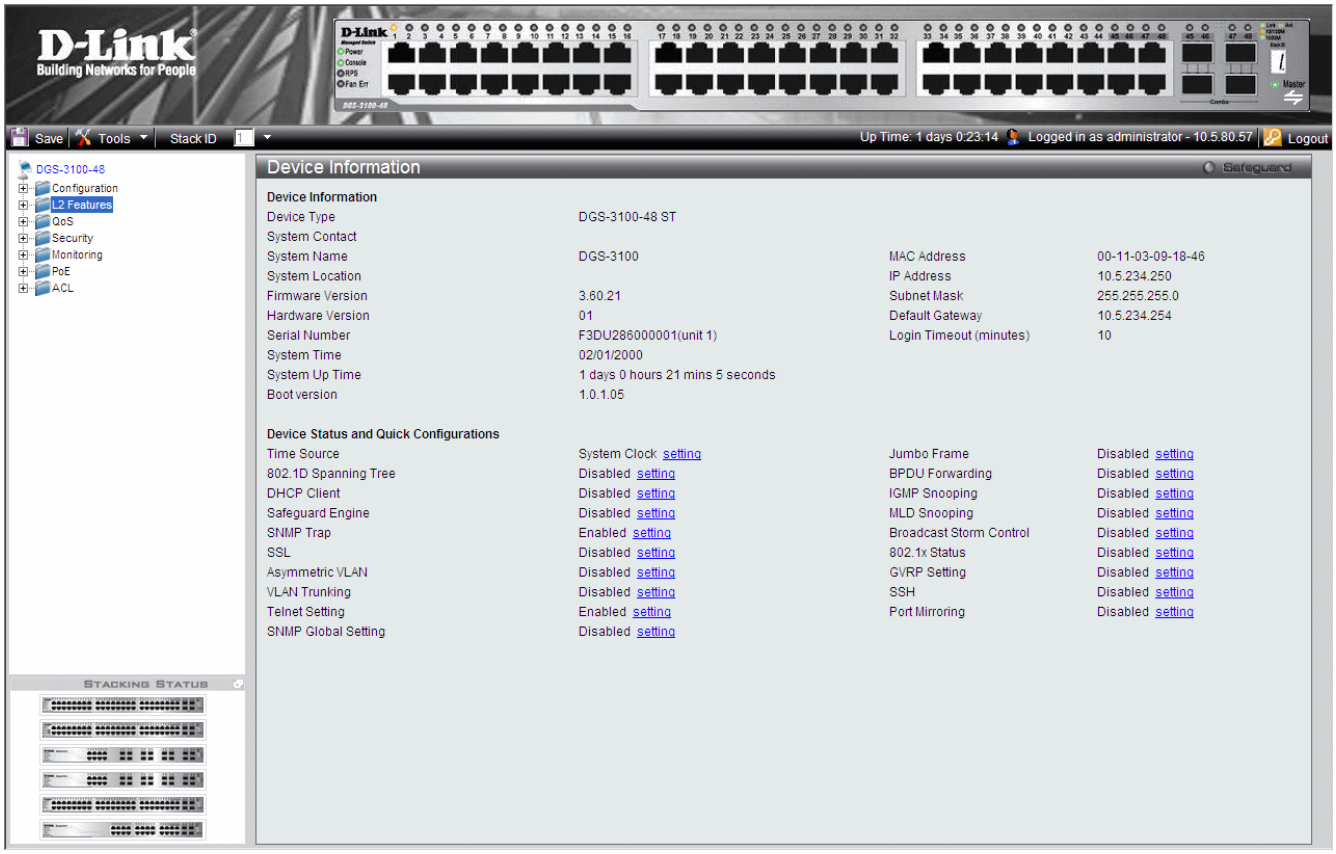


Figure 0-1 Device Information Page

The Device Information Page contains the following fields:

Field	Description
Device Type	Displays the factory defined device name and type.
System Contact	Displays the name of the contact person. The field range is 0-31 characters.
System Name	Displays the user-defined system name. The field range is 0-31 characters.
System Location	Displays the location where the system is currently running. The field range is 0-31 characters.
Firmware Version	Displays the installed software version number.
Hardware Version	Displays the installed device hardware version number.
Serial Number	Displays the installed device serial number.
System Time	Displays the system time. The field format is Day/Month/Year.
System Up Time	Displays the amount of time since the most recent device reboot. The system time is displayed in the following format: Days, Hours, Minutes, and Seconds. For example, 41 days, 2 hours, 22 minutes and 15 seconds.

Field	Description
Boot Version	Displays the installed device boot version number.
MAC Address	Displays the MAC address assigned to the device.
IP Address	Displays the IP address assigned to the device.
Subnet Mask	Displays the subnet mask assigned to the device.
Default Gateway	Displays the device default gateway assigned to the device.
Login Timeout (minutes)	Indicates the amount of time after which if no user activity occurs, the device times out. The default is 10 minutes.
Time Source	Provides a shortcut to viewing the system clock settings.
802.1D Spanning Tree	Indicates if STP is enabled on the device, and provides a shortcut to viewing the STP settings.
DHCP Client	Indicates if DCHP Client is enabled on the device, and provides a shortcut to viewing the DHCP Client settings.
Safeguard Engine	Indicates if the Safeguard Engine is enabled on the device, and provides a shortcut to viewing the Safeguard Engine settings.
SNMP Trap	Indicates if SNMP Traps are enabled on the device, and provides a shortcut to viewing the SNMP Traps settings.
SSL	Indicates if Secure Socket Layer (SSL) is enabled on the device, and provides a shortcut to viewing the SSL settings.
GVRP Setting	Indicates if Group VLAN Registration Protocol is enabled.
Telnet Setting	Indicates if Telnet is enabled.
Jumbo Frame	Indicates if Jumbo Frames are enabled on the device, and provides a shortcut to viewing the Jumbo Frames settings.
BPDU Forwarding	Indicates if BPDU Forwarding is enabled on the device, and provides a shortcut to viewing the BPDU Forwarding settings.
IGMP Snooping	Indicates if IGMP Snooping is enabled on the device, and provides a shortcut to viewing the IGMP Snooping settings.
MLD Snooping	Indicates if MLD Snooping is enabled on the device, and provides a shortcut to viewing the MLD Snooping settings.
Broadcast Storm Control	Indicates if Broadcast Storm Control is enabled on the device, and provides a shortcut to viewing the Broadcast Storm Control settings.
802.1X Status	Indicates if 802.1X is enabled on the device, and provides a shortcut to viewing the 802.1X settings.
SSH	Indicates if Secure Shell Protocol (SSH) is enabled on the device, and provides a shortcut to viewing the SSH settings.
Port Mirroring	Indicates if Port Mirroring is enabled.

To view settings for a device feature:

1. Select a device feature under the *Device Status* and *Quick Configuration Section*.
2. Click setting next to the feature name. The configuration page for the selected device feature opens**.**

Defining System Information

The *System Information Page* provides device information about specific stacking members. To view system information:

1. Click **Configuration > System Information**. The *System Information Page* opens:

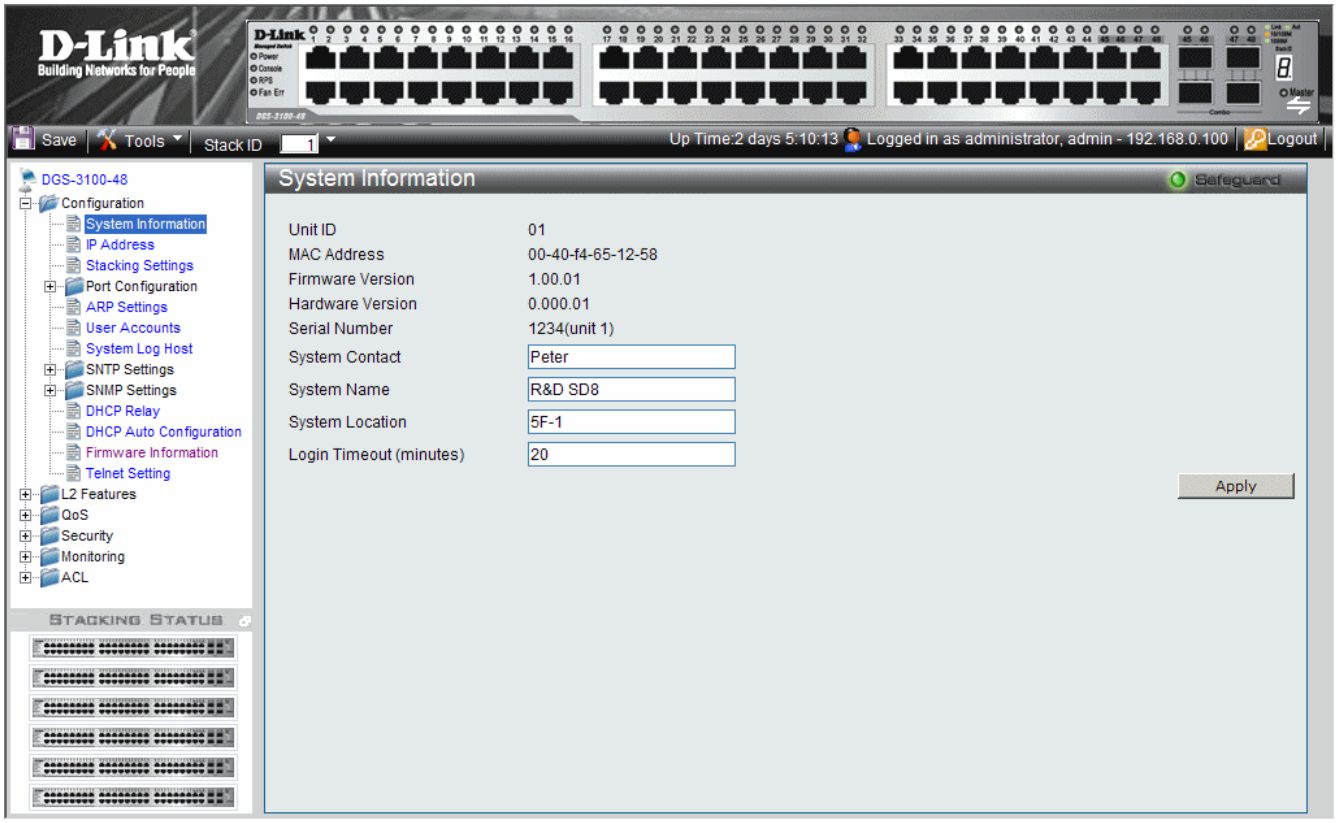


Figure 0-2 System Information Page

The System Information Page contains the following fields:

Field	Description
Unit ID	Displays the stack unit ID.
MAC Address	Displays the MAC address assigned to the device
Firmware Version	Displays the stacking member's software version number.
Hardware Version	Displays the stacking member's hardware version number.
System Contact	Defines the name of the contact person. The field range is 0-160 characters.
System Name	Defines the user-defined system name.
System Location	Defines the location where the system is currently running. The field range is 0-160 characters.
Login Timeout (minutes)	Defines the amount of time the device times out when no user activity occurs. The default is 10 minutes.

2. Define the *System Name* field.
3. Define the *System Location* and *Login Timeout (minutes)* fields.
4. Click Apply. The system information is defined, and the device is updated.

Defining IP Addresses

The *IP Address Page* contains fields for assigning IP addresses. Packets are forwarded to the default IP when frames are sent to a remote network via the *Default Gateway*. The configured IP address must belong to the same IP address subnet of one of the IP interfaces. The *Dynamic Host Configuration Protocol* (DHCP) assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices can have a different IP address every time the device connects to the network.

1. Click **Configuration > IP Address.** The *IP Address Page* opens:

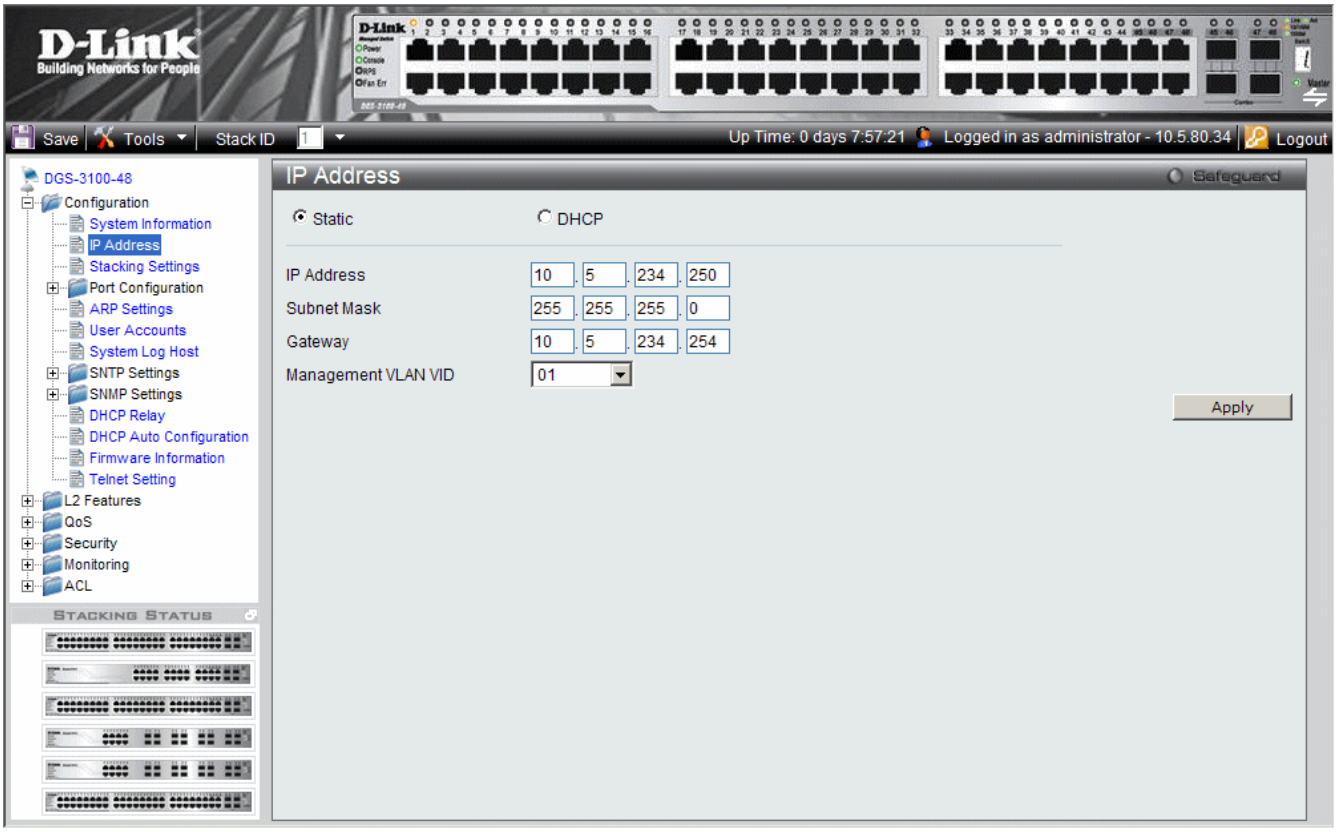


Figure 0-3 IP Address Page

The IP Address Page contains the following fields:

Field	Description
Static	When selected, the IP address is static and user-defined in the *IP Address* field. This is the default value.
DHCP	When selected, the IP address is retrieved from a DHCP server.
IP Address	Defines the IP address. This field is active if the IP address is static.
Subnet Mask	Defines the address mask that manages sub-netting on the network. The default value is 255.0.0.0.
Gateway	Defines the default gateway. The default gateway manages connections to other subnets and other networks.
Management VLAN VID	Defines the management VLAN's VID.

2. Select the IP address type in either the Static or DHCP fields.
3. If *Static* is the defined IP address type, define the *IP Address* field.
4. Define the *Subnet Mask*, *Gateway*, and *Management VLAN VID* fields.
5. Click Apply. The IP address information is defined, and the device is updated.

Managing Stacking

Stacking enhances network flexibility by building virtual switches with more ports then are available in a single device. Stacks are managed by stacking member which called *Stack Master.*, All other stacking members serve as ports only.

The following paragraphs provide a stacking explanation for DGS-3100 series and include the following topics:

- Managing Stacking Modes
- Advanced Stacking
- Building Stacks – Quick Start
- Stack Management Examples
- Configuring Stacking

Managing Stacking Modes

A switch operates in the following modes:

NOTE: The DGS-3100 series family stacking connections have two HX ports.

- **Stacking** - Switches operating in Stack mode run as organized group of switches known as a Stack. A stack consists of one Stack Master, a Backup Master, and up to four Stack Member Switches. However, in specific scenarios, a single unit can be considered a *Stack of One*. A *Stack of One* is a single unit which is not connected to any other stacking members.

If the unit is reset to the factory defaults, the unit is reloaded in stacking Auto-Numbering mode.

Advanced Stacking

This section provides information for understanding advanced stacking concepts, including:

- Unit ID and how they are allocated
- Stacking member start up process.

This section contains the following topics:

- Allocating Unit IDs
- Assigning Unit IDs

Allocating Unit IDs

Switches are shipped from the factory without a Unit ID and in *Auto Assign* mode. All switches must be assigned a Unit ID before switches can operate as stacking members. More than one stacking member cannot receive the same Unit ID. Unit IDs are assigned by:

- Assigned by the system administrator. Unit IDs that are assigned by the system administrator and can only be changed manually by the system administrator.
- If the system administrator does not set the Unit IDs manually, the Auto Assign initializes the switches when they are powered up. From the switches who are automatically assigned a Unit ID, one of the stacking members is assigned the Unit ID 1. That stacking member is the Stack Master. If there were more than one switch in the stack, there is a Master Election and Backup Master Election process. Following the Master Election process, the other stacking members are assigned a Unit ID by the stack Master. For more information on the Master Election process, please see *Electing a Stacking Master*.

Stacking members maintain the assigned Unit ID even after the stacking member is rebooted. The Stack Master may reallocate IDs during system initialization to resolve duplicate ID conflicts. Manually assigned IDs cannot be changed by the Stack Master, even if there is a conflict.

Unit ID assignments or modifications are effective only during system initialization, and do not occur during the system up-time.

Stacking members do not have to be numbered in sequence, and can be interconnected, as long as each stacking has a unique ID, and at least, one stacking member serves as the Stack Master.

Assigning Unit IDs

Each stacking member has an assigned unique Unit ID. Unit ID numbers are assigned as follows:

- **Unit ID 1** - Assigned to the Stack Master. The Stack Master is indicated by the Master LED on front which is lit solid green.
- **Unit ID 2** - Assigned to the Backup Master
- **Unit ID 3, 4, 5, and 6** - Assigned to Stacking members.

NOTE: There are cases in which a unit to which Unit ID 1 is assigned is not the stack Master but a Backup Master.

This section contains the following topics:

- Defining a Stacking Master
- Defining a Stacking Back Up Master
- Defining Stacking Members
- Master Enabled Stacking Members
- Electing a Stacking Master

Defining a Stacking Master

The stacking member assigned the Unit ID1 operates as the *Stack Master*.

The Stack Master provides a single point of control, configuration, and management for the entire stack. In addition, the Stack Master stores all stack member configuration. The individual stacking members do not store any configuration information.

Defining a Stacking Back Up Master

The stacking member assigned the Unit ID 2 is defined as the stack's Backup Master.

In addition to being a stack member, Backup Master serves as a backup in case the Stack Master fails or disconnected. If the Stack Master fails or disconnected, the Backup Master takes over as the Stack Master.

The Stack Master stores an active configuration which copied on the Backup Master. The active configuration copy is used if the Backup Master takes over for the Stack Master. Only the configuration file is copied. Any dynamically filled tables, for example, learnt address, are not copied from the Stack Master to the Backup Master. If the Backup Master takes over the role of Stack Master, the Backup Master builds new dynamic tables.

Defining Stacking Members

Switches assigned the Unit IDs 3,4,5,6 are called stacking members. The Stack Master (or Backup Master if the Stack Master fails) manages the stack members operation. Stacking members cannot be directly managed or configured. If neither the Stack Master nor the Backup Master were operating, the stacking members cannot function.

Master Enabled Stacking Members

Only Stacking members assigned to Unit ID 1 or 2 are called Master Enabled stacking members. Only the Master Enabled stacking members participate in the Master Election process, and therefore can become master or backup master (that means the s with assigned IDs of 3, 4, 5 and 6 can never become neither a master nor a backup master unless their ID is changed by the system administrator or reset to the factory default firstly).

Electing a Stacking Master

Whenever a stacking member (or more than one) comes up, one of the stacking members is elected to be the stack Master. The Stack Master is selected as follows:

- If one of the master enabled stacking members in the stack was set to *Force Master* by the system administrator (through the GUI – Stacking Master selector), that master enabled stacking member is the Stack Master. Stacking

members which are defined as *Force Master* stacking members are manually selected as the Stack Master. Only a master enabled stacking member can be selected as the *Force Master*.

- If the stack contains more than one stacking member whose Unit ID is either 1 or 2, then one of the stacking members are elected the Stack Master. It does not matter if the Unit ID was originally automatically or manually assigned. These stacking members are called *Master Enabled*. If there is only one stacking member, that stacking member is selected as the Stack Master, even if the stacking member's Unit ID is 2. If there is a stacking member Unit ID 2 which up-time is 30 minutes and Unit ID 1's uptime is 19 minutes. The difference is 11, which is greater than 10 minutes, thus the Unit ID 2 is the elected Stack Master.
- If there are more than one stacking members, the two stacking members decide which stacking member is elected Stack Master by checking:
  - Which stacking member has been running for a longer time. The up-time is measured in increments of 10 minutes. The stacking member running the longest is elected the Stack Master.
  - If they have been running for the same amount of time, the stacking member with the Unit ID 1 is the stack Master.
  - If both stacking members have been running for the same amount of time, and both stacking membes have the same Unit ID, the stacking members with the lowest MAC addressis selected as the Stack Master. The other unit is rebooted and is assigned the Unit ID 2.
  - If the stack contains one or more stacking members set to the factory default states, and there is no Unit ID assigned to a stacking member, then the Stack Master is one of these stacking members. The stacking member selected to be the Master is the stacking member running for the longest time. If all stacking members are running the same amount of time, the stacking member with the lowest MAC address is selected as the Stack Master.

The Master Election results in an elected Stack Master. The Stack master has a Unit ID of 1 and the Backup Master has a Unit ID of 2 (if a Backup Master was included in the stack).

If a Master Enabled stacking member, a Unit ID of 1 or 2, is added to a stack and powered on, the newly added switch invokes Master Election process. The Master Election process occurs even though the stack has an elected master. However, the newly added switch loses in the election process (lower up-time) and joins the stack as a stacking member or Backup Master.

Stack Startup Process

When a stacking member is initialized, either powered up or rebooted, the stacking member goes through the same exact process including:

- Discovering the Stacking Master.
- Allocating Unit IDs/Resolving Unit ID Conflicts
- Unit and Stacking Port Configuration

Discovering the Stacking Master

When a stacking member is initialized in stack mode, the stacking member's behavior depends on its Unit ID.

- If the stacking member does not have a current Unit ID the stacking member operates in *Factory Default* mode. If there is a Stacking Master, the stacking member is assigned a Unit ID through Unit ID Allocation. The stacking members receive a Unit ID from the Stacking Master. If the stack does not have a Stacking master then the switch participates in Master-Election, and may be elected either the new Stacking Master or Backup Master.
- If the stacking member's current Unit ID is 1 or 2, the stacking member participates in the Master Election. For example, the Unit ID was previously allocated, or the stacking member was in a different stack.
- If the stacking member has a current Unit ID the stacking members attempts to use the Unit ID in the new stack. If the stacking member current ID is 3, 4, 5, or 6, then the stacking members attempts to connect to the running Stack Master. The new stacking member does not proceed to the next stage until there is contact with the Stack Master. These stacking members do not participate in the *Master Election* process, and if no Stack Master is present, the stacking members' network ports are shut down. Only the stacking ports are operational.

Both the Stack Master and all other stacking members carry out a continuous process of *Master Discovery* by frequently exchanging stack control messages. This allows the stacking members to discover when a stacking member fails or is unreachable.

Allocating Unit IDs/Resolving Unit ID Conflicts

Once the Stack Master is elected, it allocates the Unit IDs to the stacking members that do not have a Unit ID. Stacking members that do not have a Unit ID operate in the *Factory Default* mode.

In addition, the stack Master attempts to resolve all duplicate Unit IDs occurrences among stacking members. The Stack Master reallocates the duplicate Unit ID if there are available Unit IDs.

If two stacks are merged, stacking units that were initially in the Stack Master's sub-group retain their Unit ID. New stacking member are allocated new Unit IDs.

If a conflict occurs after the stacking members are rebooted, the following occurs:

- If both duplicate stacking members are in *Auto Assign* mode, then the Unit ID is assigned by the MAC address. The stacking member with the lowest MAC address maintains its Unit ID. The other stacking member is assigned a new Unit ID.
- If one of the stacking members with duplicate Unit IDs is in *Auto Assign* mode and the other stacking member is in manual mode, the stacking member in *Manual* mode maintains its Unit ID, The other stacking member is assigned a new Unit ID. .

Stacking members are shut down if:

- If both duplicate stacking members are in *Manual* mode then both stacking members are *shut down*.
- If the Stack Master is able to allocate a Unit ID to each stacking member, then all stacking members operate as a stack. If the Stack Master is unable to allocate a Unit ID to any stacking member, that stacking member is effectively *shut down* and does not participate in the stack.
- Stacking members with a conflicting manually set ID are shut down as the Stack Master cannot override the system administrator's Unit ID assignment to resolve the conflict.
- If there are more stacking members than the maximum number allowed in a stack, and the incoming stacking members are already in *Factory Default* mode, the Stack Master is elected following *Master Discovery* and *Master Election* processes. All other stacking members are shut down in some extreme cases, due to during the boot process, where some stacking members may be connected and join the stack. If the new stacking members are already assigned a Unit, then the new stacking members cannot join the stack. The switches are remains shut down.

If a stacking member is shut down, the stacking members stacking links are inactive. Moreover, if the stacking members are connected in a chain topology, the shut down of one stacking member breaks the chain. This may cause other stacking members to be disconnected and shut down if the stacking members have no active link to the Stack Master.

Unit and Stacking Port Configuration

Each stacking member has a Unit ID; one of the stacking members is the stack Master, and, possibly, one of the stacking members serves as Backup Master. The Stack Master now configures each stacking member according to the Configuration file stored on the Stack Master.

If the stack has a Backup Master the Configuration file are also be copied to the Backup Master.

Once all the stacking members are configured, the stack proceeds to a normal operational mode. If any change is made to the system configuration, the change is stored by the stack Master and is copied to the Backup Master.

Building Stacks – Quick Start

The DGS-3100 series supports the following stacking scenarios:

- Building a new stack from scratch
- Increasing the stack by adding units to an existing stack

This section contains the following topics:

- Stack Resiliency
- Managing a Self-Ordered Stack
- Managing a New Manually Ordered Stack

Stack Resiliency

Topologies of stack can be either Ring or Chain. Best practice is to configure the stack in Ring topology, due to the high resiliency in case of unit failure or stacking link failure.

Additionally, in case of redundant power supply usage it is recommended to make sure that Master and Backup Master s are connected to a redundant power supply.

Managing a Self-Ordered Stack

This section describes managing a self-ordered stack. Self–ordered stacks are automatically assigned Unit IDs by the system through the Master Election process. This section contains the following topics:

- Building a New Self-Ordered Stack
- Adding Members to a Self Ordered Running Stack

Building a New Self-Ordered Stack

To build a self ordered stack:

1. Connect the units physically through the stacking ports.
2. Turn on the units. After a short interval the stack will become operational with one of the units selected as the Master of the stack. The Master and Backup selection is known as *Master Election*. Master Election takes place if there are one or more eligible candidates contending to be the Master unit. The Master Unit is indicated by the green Master LED on the front panel. The Master LED is located near the Unit ID LEDs. If a serial console is connected, the serial cable must be connected to the Stack Master console port since the only operational console port in the stack is the one of the Master unit**.**

NOTE: To reset the stacking members to the factory defaults, press the Reset button for at least 5 seconds.

Adding Members to a Self Ordered Running Stack

1. Reset the new stacking units to the factory defaults by pressing the Reset button (optional).
2. Connect the stacking members physically to the stack.
3. Turn on the switches, the new units will become stacking members**.**

Managing a New Manually Ordered Stack

System administrator can also manually assign Unit IDs to stacking members. System administrator has to assign a unique Unit ID from 1 to 6 to each stack member.

A Unit ID that is manually assigned is not subject to automatic numbering. The Unit IDs are assigned as follows:

- **Unit ID 1** – Assigned to the Stacking Master. The Stack Master is indicated by the Master LED on front which is lit solid green.
- **Unit ID 2 -** Assigned to the Backup Master
- **Unit ID 3 4, 5, 6 –**Assigned to the Stacking member.

This section contains the following topics:

- Building New Manually Ordered Stacks
- Adding Stacking Members to an Existing Manually Ordered Stack

Building New Manually Ordered Stacks

To build new a self ordered stack:

1. Connect the units physically through the stacking ports.
2. Turn on the units, one at a time.
3. Assign the Stack Master the Unit ID of 1 using a Stack Management Interfaces either the console port, Telnet, or Embedded Web Interface.
4. Assign the Backup Master the Unit ID of 2 using a Stack Management Interfaces either the console port, Telnet, or Embedded Web Interface.
5. Assign the remaining stacking members using a Stack Management Interfaces either the console port, Telnet, or Embedded Web Interface.
6. Ensure that none of the stacking members have the same Unit ID.
7. Reboot all the stack units.

Adding Stacking Members to an Existing Manually Ordered Stack

To add units to an existing manually ordered stack:

1. Reset the new stacking units to the factory defaults by pressing the *Reset* button.
2. Connect the stacking members physically to the stack.
3. Turn on the switches, the new units become stacking members, but with automatically assigned Unit IDs.
4. Reassign the Unit ID manually to each of the newly added stacking members using a Stack Management Interfaces either the console port, Telnet, or Embedded Web Interface. This step is optional, and the stack is operational even if some unit IDs were manually configured while others are self-assigned.
5. Reboot the stacking members to ensure the Unit ID is permanent.

Stack Management Examples

This section contains information for troubleshooting stacking, and includes the following topics:

- Replacing Failed Stacking-Members in a Running Stack
- Replacing a Failed Stack Master
- Dividing Stacks
- Merging Stacks
- Stacking Cable Failure
- Inserting Excess Stacking Members

Replacing Failed Stacking-Members in a Running Stack

This example assumes that a stacking member, other than master, has failed in a running stack, when the system administrator is notified of the system failure the stacking member is removed and replaced with a new switch.

When the stacking member fails, the Stack Master identifies the failed stacking member using the *Master Discovery* process. The Stack Master recognizes that the stacking member no longer responds. If the stack topology was ring topology, the Stack Master directs all other stack members to route traffic around the failed stacking member. At the same time the Stack Master notifies the system administrator of the failure using SYSLOG messages and SNMP traps.

When the failed stacking member is disconnected from the stack, all traffic is routed around the failed stacking member as stated above. As long as all other stacking connections are intact, the stack continues to run.

When a new stacking member is inserted and the stack is powered up, the following occurs:

- The new stacking member which is in stacking mode, performs the *Master Discovery* process, and perhaps participates in a *Master Election* .For more information on the Master Election process, see *Electing a Stacking Master*.

  - If the new stacking member has a Unit ID of *1* or *2*, i.e. the stacking member is a master enabled unit, the new stacking member initiates the Master Election process. However, since the running Stack Master has a longer up-time, it remains the Stack Master and the new stacking member does not become a new Stack Master.
  - If the new stacking member has a Unit ID of 3 to 6, the new unit attempts to become a stacking member, and is subject to the already running Stack Master. The Master Election process does not occur.
- The Stack Master performs a Unit ID Allocation and Conflict Resolution process.
  - If the new stacking member was in Factory Default mode (the unit does not have an assigned Unit ID). The new stacking member is assigned the lowest available Unit ID by the Stack Master. It is strongly recommended that automatic assigned Unit ID mode be used since it provides improved stack resiliency.
  - If the new stacking member already has an assigned Unit ID, and that Unit ID is unused in the current stack, the new stacking member retains its assigned Unit ID. The Stack Master applies any configuration relevant to that Unit ID.
  - If the new stacking member already has an assigned Unit ID, and that Unit ID conflicts with an existing Unit ID the Stack Master reallocates a new Unit ID to the new stacking member. , The lowest available Unit ID is applied to the new stacking member. This occurs only if new stacking member does not have a manually assigned Unit ID, which the Stack Master cannot change.
  - If the new stacking member cannot be assigned an available Unit ID, then the new stacking member is effectively shut down and cannot join the stack. For example, the stacking member replacement can only occur if the new stacking member has a manually assigned Unit ID.
- The Stack Master now performs Unit *and Stacking Port Configuration* for the new stacking member.
- Any configuration information which the Stack Master stores that is relevant to the Unit ID is assigned to the new stacking member. If the new stacking member was assigned the same Unit ID of the replaced stacking member, then the new stacking member receives the same configuration as the failed stacking member. If the new stacking member is identical to the replaced stacking member, the entire configuration of the replaced stacking member is applied to the new stacking member. The stack reverts to the stacking state it was running in before stacking member failed. However, sometimes the new stacking member is not identical to the failed stacking member. The Stack Master applies the configuration as follows:
- If a 24-port switch replaces a failed 48-port switch, then the new stacking member's ports are configured according first 24 ports configuration of the failed stacking member.

NOTE: The 48 port configuration of the failed stacking member is recorded, even though only the first 24 port configuration is currently applied. If a 48 port switch is inserted and assigned the same Unit ID, the switch is configured with the port configuration of the original 48 port stacking member.

- If a 48-port stacking member replaces a 24-port stacking member, then the first 24 ports of thenew stacking member are configured according failed stacking member's ports configuration. The remaining new stacking member ports are configured with the switch's default settings.

Replacing a Failed Stack Master

This example assumes that that a stacking member acting as the Stack Master has failed in a running stack. When the system administrator is notified of the Stack Master failure and replaces existing Stack Master with a new switch.

When the Stack Master fails, the stack's Backup Master recognizes the failure and that the Stack Master no longer responds and assumes the role of Stack Master. The Backup Master uses Master Discovery process to identify the failure. In case of Ring topology the Backup Master directs all other stack members to route traffic around the failed stacking member. At the same time the Backup Master notifies the system administrator of the failure using SYSLOG messages and SNMP traps.

When the failed stacking member is disconnected from the stack, all traffic is already routed around the failed stacking member. If all other stacking connections are left intact, the stack keeps running. When a new stacking member is inserted and powered up, the following occurs:

- The new stacking member performs *Master Discovery* process, and participates in a Master Election process. For more information on the Master Election, see *Electing a Stacking Master*.
  - If the new stacking member has a Unit ID of *1* or *2*, i.e. the stacking member is a master enabled; Master Election process is initiated. Since the running stack Backup Master has a longer run timeand if the Backup Master has been running for more then 10 minutes, the Backup Master remains the elected Stack Master. The new stacking member does not become the new Stack Master. This may result in new stacking member using

Unit ID 1, and serving as the stack Backup master, while the already running stacking member with Unit ID 2 remains the active Stack Master.

- The Stack Master performs Unit ID Allocation and Conflict Resolution process.
  - If the new stacking member is in the *Factory Default* mode, the new stacking member is assigned the lowest available Unit ID by the Stack Master. It is strongly recommended that *Auto Assign* mode is used to assign the Unit ID. The *Auto Assign* mode provides better stack resiliency.
  - If the new stacking member already has an assigned Unit ID, and that Unit ID is unused in the current stack, the incoming stacking member is assigned Unit ID. The Stack Master applies any device configuration to the new stacking member.
  - If the new stacking member already has an assigned Unit ID, and that UnitID conflicts with an existing Unit ID the Stack Master reallocates a new Unit ID to the new stacking member. The lowest available Unit ID is applied to the new stacking member. This occurs only if new stacking member does not have a manually assigned Unit ID, which the Stack Master cannot change.
  - If the new stacking member cannot be assigned an available Unit ID, then the new stacking member is effectively shut down and cannot join stack. For example, if stacking member replacement that can only occur if the new stacking member has a manually assigned Unit ID.
- The Stack Master performs Unit *and Stacking Port Configuration* for the new stacking member.
- Any configuration information the Stack Master retains that is relevant to the Unit ID of the new stacking member is applied. If the new stacking member was assigned the same Unit ID of the replaced stacking member, then the new stacking member receives the same switch configuration as the failed stacking member, described in *Replacing Failed Stacking-Members in a Running* Stack.

Dividing Stacks

This example assumes that a working stack is divided into two groups. The stack is divided either by a failed stacking link connected to two stacking members in the stack or by a failed stacking members in a chain topology which causes disconnection between two units in the stack. In this case we should consider each sub-group as an independent running stack configuration. For each sub-group we should consider three sub options:

- Both the Stack Master and the Backup Master are part of the sub-group.
- Either the Stack Master or the Backup Master is part of the sub-group.
- Neither the Stack Master nor the Backup Master is part of the sub-group.

When a stack is split into two parts, the following occurs in each partial stack according to the following scenario:

Both the Stack Master and the Backup Master are part of the sub-group.

Nothing changes, except the Stack Master recognizes the missing stacking members as removed stacking members and routes traffic around them.

Since both the Stack Master and Backup Master are in this stacking section, this section is operating and the other section cannot operate.

The following occurs when the stack is divided and both the Master and Backup master are in the sub-group:

- The Master Discovery, Master Election and Unit ID Allocation & Duplicate Unit ID Conflict Resolution processes are performed, resulting in the following:
  - Any configuration information stored by Stack Master, which remained in the group, that is relevant to the stacking members remains unchanged.
  - Topology information, inter-stacking member forwarding information for transmitting traffic to any other stacking member, managed by the Stack Master includes only stacking members that remain connected after the stack is divided.
  - The divided stack continues to operates normally, the only difference is there are less stacking members than prior to the stack division.
  - No Unit ID changes are performed in each divided stack.
  - The Stack Master notifies the system administrator using SYSLOG messages and SNMP traps of the removed stacking members. In addition the Stack Master also notifies the system administrator whichd ports belong to unreachable stacking members and are reported as *Not Present*.
- Either the Stack Master or the Backup Master remain in the divided group

- If the Stack Master remains in this sub-group, the behavior is the same as described above. If the Backup Master remains in this sub group the behavior is the same as described in0 - *Replacing a Failed Stack Master* .

NOTE: **If a stack is divided into two parts with one section which containing the Stack Master, and the other section - Backup Master w**as operate.

The following occurs if either the Stack Master or the Backup Master remains in the divided group:

- The *Master Discovery*, *Master Election* and *Unit ID Allocation & Duplicate Unit ID Conflict Resolution* processes are performed, resulting in the following:
  - When the stack is divided and if the Stack Master remains in the split stack, the Stack Master recognizes that the stacking units were no longer responds. This occurs using the *Master Detection Process*. The Stack Master notifies the system administrator using SYSLOG messages and SNMP traps of the removed stacking members. In addition the Stack Master also notifies the system administrator whichd ports belong to unreachable stacking members and are reported as *Not Present*.
  - if the Backup Master remains in the split stack, when the stack is divided, the Backup Master identifies this as of the Stack Master failing. The Backup Master takes over and manages the remaining stacking members as a stack. The Backup Master retains the same Unit ID as before the stack was divided. Since the Backup Master was not acting as the Stack Master prior to the split, the Back Master initiates a Topology Database and port learning process. Traffic can be halted for a short period until the stack is synchronized, i.e., stacking member and port configuraiton is completed. New stacking members are learnt by the Backup Master are notified to the system administrator using SYSLOG messages and SNMP traps.
  - The divided stack continues to operate normally, the only difference is there are less stacking members than prior to the stack division.No Unit ID changes are performed in each the divided stacks.
  - Even if each stacking section has a Stack Master, one section retains the Stack Master and the other section the Backup Master, both stacks have the same configuration and the same IP address.

NOTE**:** If both stacks have the same IP Address, this can lead to network problem. There is no way for users to connect to any stacks through the stack IP address

If neither the Stack Master nor the Backup Master remain in the divided group.

- This is identical to failed Stack Master, where no backup is available.
- Stacking members whose Unit IDs are 3, 4, 5 or 6 in original stack do not renumber themselves. The stacking members' network ports remains shut down until a Stack Master is enabled, is connected and is operating as the Stack Master .The Master-Discovery process recognized that the Stack Master has been separated from the stack.
- The stacking members lose connection with the Stack Master. Since the stacking members started as a running stack, and the stacking members are not in the Factory *Default Mode*, the stacking members are not reassigned Unit IDs. Resetting the stacking members will initiate Unit ID auto-assignment. No Unit ID changes are performed in each one of the two stacking sections of the original stacks.

NOTE: None of the stacking members in either stacking sections can remember themselves.

Merging Stacks

This example assumes that the user would like to merge two working stacks. This creates one stack from two separate stacks. There are two scenarios:

If new stacking members are powered down during insertion and then powered up

- This is identical to insert stacking members into a running stack, see *Replacing Failed Stacking-Members in a Running Stack*. The only difference is that an additional stacking member is inserted into the stack. Therefore, for each stacking member inserted the same process occurs.

If stacks being merged are connecting via stacking cables and, both stacks are running the following occurs:

- If each of the joined stacks has a Stack Master, both Stack Masters s perform the *Master Discovery* process. Both Stack Masters participate in the *Master Election* process. One Stack Master is selected as the Stack Master. The criteria for selecting a Stack Master in a merged stack as follows:
  - Force Master
  - System Up Time
  - Lowest Unit ID
  - Lowest MAC Address
- The process of master selection between two Stack Masters is as follows:
  - If Force Master is enabled, then the Stack Master which was forced is selected.
  - The *System Up Time* is measured in increments of 10 minutes The Stack Master with longest System Up Time is selected as Stack Master.
  - If both Stack Masters have the same *Up Time,* the Stack Master with the lowest Unit ID is selected as Stack Master.
  - If both Stack Master Unit IDs are equal the Stack Master with the lowest MAC address is selected.
  - The Master Election process assigns a dynamically allocated Unit ID Reassignment of Unit Id to the other Stack Master and is performed by the new Stack Master. The switch is either allocated as a stack memberor the Backup Master. There cannot be two stacking members with the same Unit ID at the process end.
  - The Stacking Master that loses the Master election process is shut down if the Unit ID was manually allocated. It is recommended that the administrator configure the switch to *Auto Assign* mode before reconnecting the switch to the stack.
  - When two stacks are combined, all of the configuration information for one of the stacks is lost. After the discovery/election process is completed, only the new Stack Master maintains its configuration information,
  - If one of the merged stacks had neither a Stack Master unit nor a Backup Master, then stacking members belonging to this groupare inserted into the stack as in *Replacing Failed Stacking-Members in a Running Stack*. The Stack Master either connects stacking members to the stack using thecurrent Unit Ids or reallocates the Unit IDs necessary. For more information see *Replacing Failed Stacking-Members in a Running Stack*.

If two stacks are merged into one stack, both stack configuration cannot be to maintained. All stacking member's dynamic information that belong to the portion of the stack that was not reelected is lost and the new Stack Master relearns the information. .

Stacking Cable Failure

This example assumes that S*tacking Connection Cables* failed and caused the stack to split, as described in *Dividing Stacks*. When the stacking cable connection is fixed and stacking members are reconnected, it results in merging two stacks as described in *Merging Stacks*.

This can be occured only if the topology of the stack is *Chain* topology. Single stacking cable failure does not causes a stack split if a *Ring* topology is used.

Inserting Excess Stacking Members

This example assumes that the user attempts to insert too many stacking members into s into a stack.

- All stacking members (existing and newly inserted) are powered on at the same time:
  - A Stack Master is elected following *Master Discovery* and *Master Election* processes.
  - All excess stacking members are shutdown.

- A running stacking member group is added to an existing stack, assuming each one of the stack groups has an elected Stack Master. The total of existing stacking members and new stacking members exceeds the maximum allowed number of stacking members in a stack, which is 6 stacking members:
  - *Master Detection* and *Master Election* processes determine the master out of one of two combined stacking groups.
  - When switches are added to a running stack, the *Unit ID Allocation and Duplicate ID Conflict Resolution* process detects an error if too many switches are present in the stack, and no changes are to stacking members that originally belonged to the group managed by the newly elected master. The original switches retain their ID assignments and configurations. The stacking members that originally belonged to the group managed by the Stack Master that lost the Master Election process are shut down.

Configuring Stacking

The *Stacking Settings Page* allows network managers to execute force master and to change each and every unit its own unit ID. To complete the changing process the user need to reboot the unit.

1. Click **Configuration > Stacking Settings.** The Stacking Settings Page opens**:**

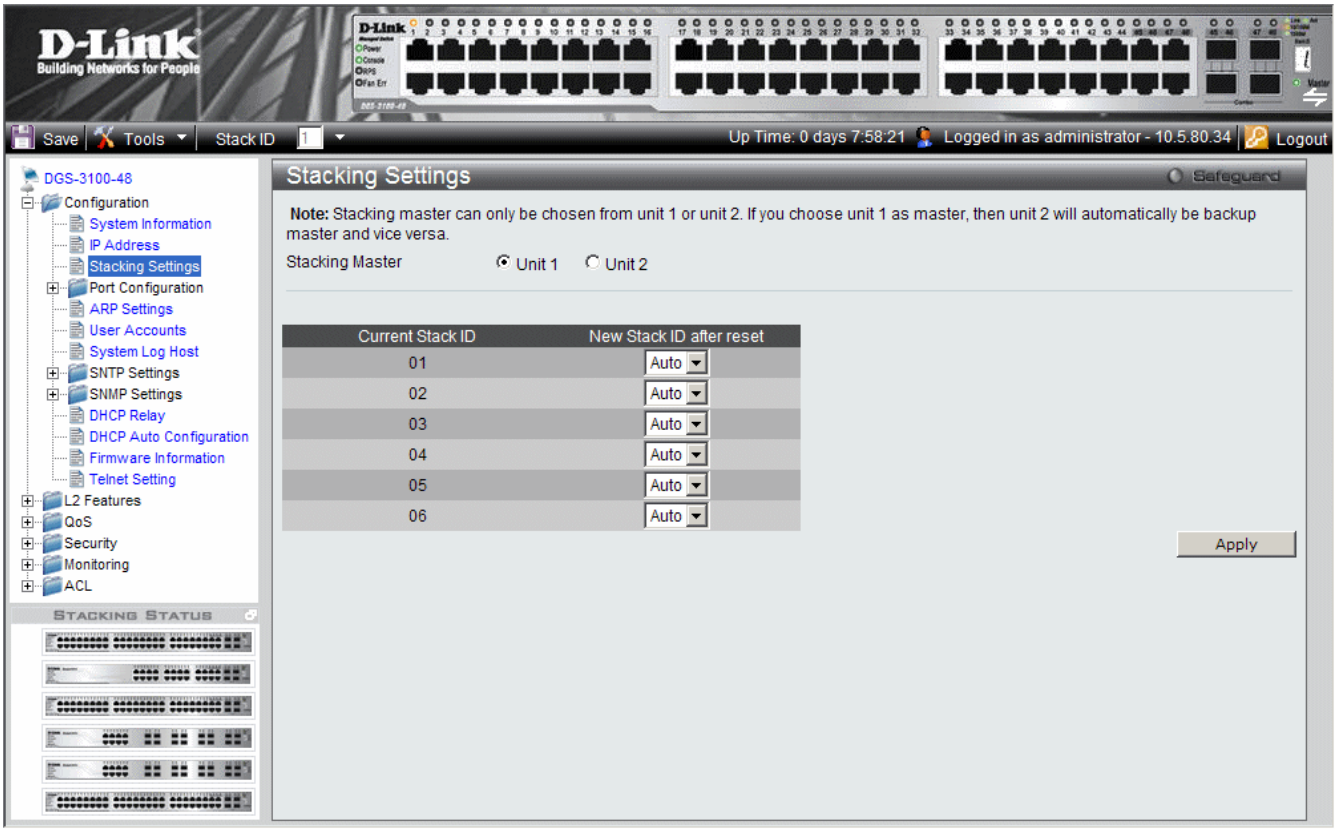


Figure 0-4 Stacking Settings Page

The Stacking Settings Page contains the following fields:

Field	Description
Stacking Master	Defines the stacking member with either stacking ID of 1 or 2 as the Stacking Master. The possible field values are: *Unit 1* — Defines the member with the Unit ID 1 as the Stacking Master if unit ID 2 will be selected unit ID 1 will be reboot and ID 2 will become stack master. *Unit 2* — Defines the member with the Unit ID 2 as the Stacking Master if unit ID 1 will be selected unit ID 2 will be reboot and ID 1 will become stack master.
Current Stack ID	Displays the Stacking Member ID that the new Unit ID will replace after the device is rboot.
New Stack ID after reset	Defines the unit ID assigned to the Stacking Member after the device rboot.

2. Select the Stacking Master in the *Stacking Master* field.
3. Select a Unit ID in the *New Stack ID after reboot* field.
4. Click Apply. If force master was selected then current master will be rebooted. If unit ID was change then the changes will be applied and occurd after the reboot.

Defining Ports

- Configuring Port Properties
- Viewing Port Properties

Configuring Port Properties

The *Port Setting Page* contains parameters for configuring port or LAG properties. Gigabit ports operate in full duplex mode only, and take on certain characteristics that are different from the other choices listed. The copper ports also support auto MDI/MDIX for cross over cables.

To define port parameters:

1. Click **Configuration >Port Configuration > Port Setting**. The *Port Setting Page* opens:

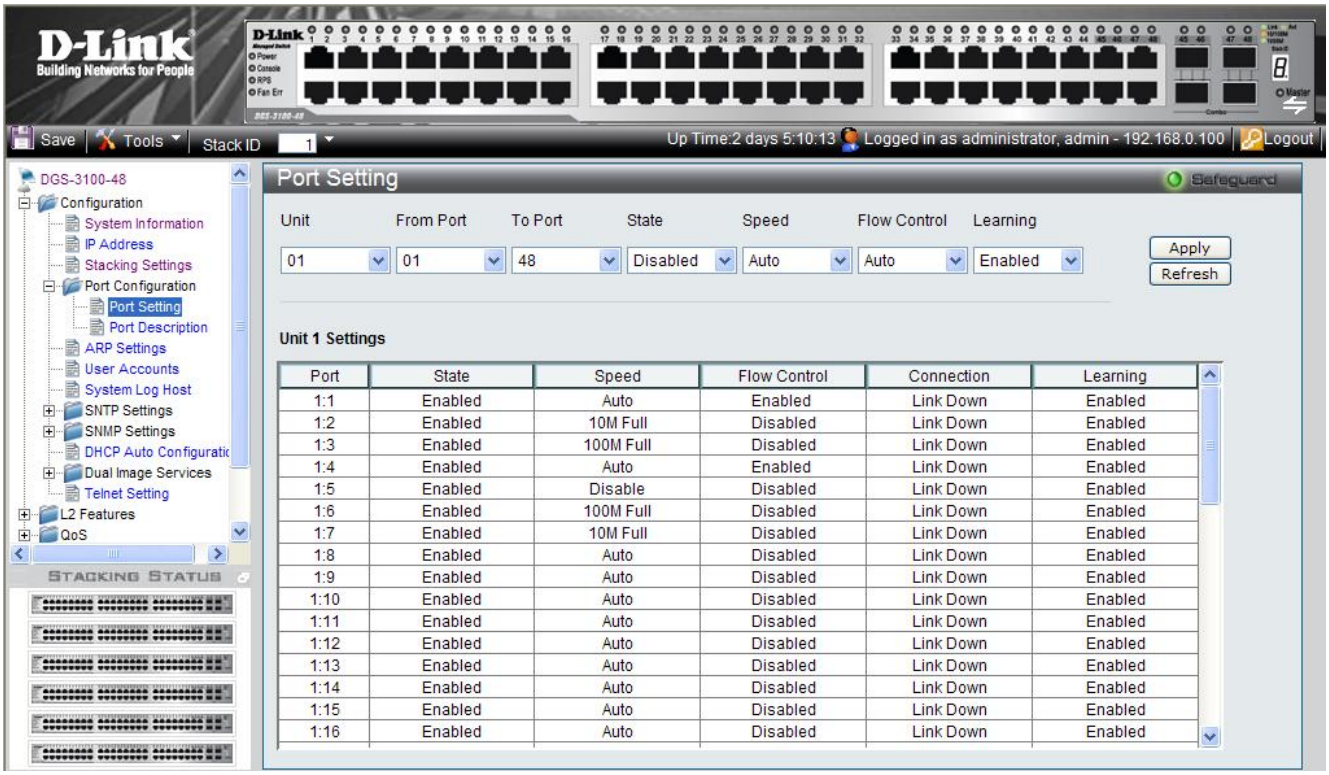


Figure 0-5 Port Setting Page

The Port Setting Page contains the following fields:

Field	Description
Unit	Defines the stacking member or LAG for which the port settings are displayed.
From Port	Defines the port number from which the port configuration will apply.. This field appears only if a unit number is selected in the Unit field.
From LAG	Defines the LAG number from which the port configuration will apply. This field appears only if LAG is selected in the Unit field.
To Port	Defines the port number to which ports the configuration will apply. This field appears only if a unit number is selected in the Unit field.
To LAG	Defines the LAG number to which the port configuration will apply. This field appears only if LAG is selected in the Unit field.
State	Defines whether the interface interface is currently operational or non-operational. The possible field values are:

Field	Description
	Enabled — Indicates that the interface is currently receiving and transmitting traffic. *Disabled* — Indicates that the interface is currently not receiving and not transmitting traffic. This is the default value.
Speed	Defines the configured rate for the interface. The port rate determines what speed setting options are available. The possible field values are: *10M/Full* — Indicates the interface is currently operating at 10 Mbps and full duplex mode. *10M/Half* — Indicates the interface is currently operating at 10 Mbps and half duplex mode. *100M/Full* — Indicates the interface is currently operating at 100 Mbps and full duplex mode. *100M/Half* — Indicates the interface is currently operating at 100 Mbps and half duplex mode. *1000M/Full* — Indicates the interface is currently operating at 1000 Mbps and full duplex mode. *Auto* —Indicates the interface is automatically configured to the fastest network traffic the interface can manage.
Flow Control	Defines the flow control scheme used for the various port configurations. Interface configured for full-duplex use 802.3x flow control, half-duplex interfaces use backpressure flow control, and *Auto* interfaces use an automatic selection of the two. The default is *Disabled*.
Learning	Defines whether MAC address learning is enabled on the ports. The possible field values are: *Enabled* — Enables MAC address learning on the interface. If MAC address learning is enabled, the source and destination MAC address are recorded in the Forwarding Table. *(*This is the default value) *Disabled* — Disables MAC address learning..

2. Define the *Unit, From Por* or *From LAG t, To Port* or *To LAG, State, Speed, Flow Control,* and *Learning* fields.
3. Click Apply. The port configuration is saved, and the device is updated.

Viewing Port Properties

The *Port Description Page* allows network managers provide a description of device ports. To define a port description:

1. Click **Configuration** > >**Port Configuration** > **Port Description**. The *Port Description Page* opens:

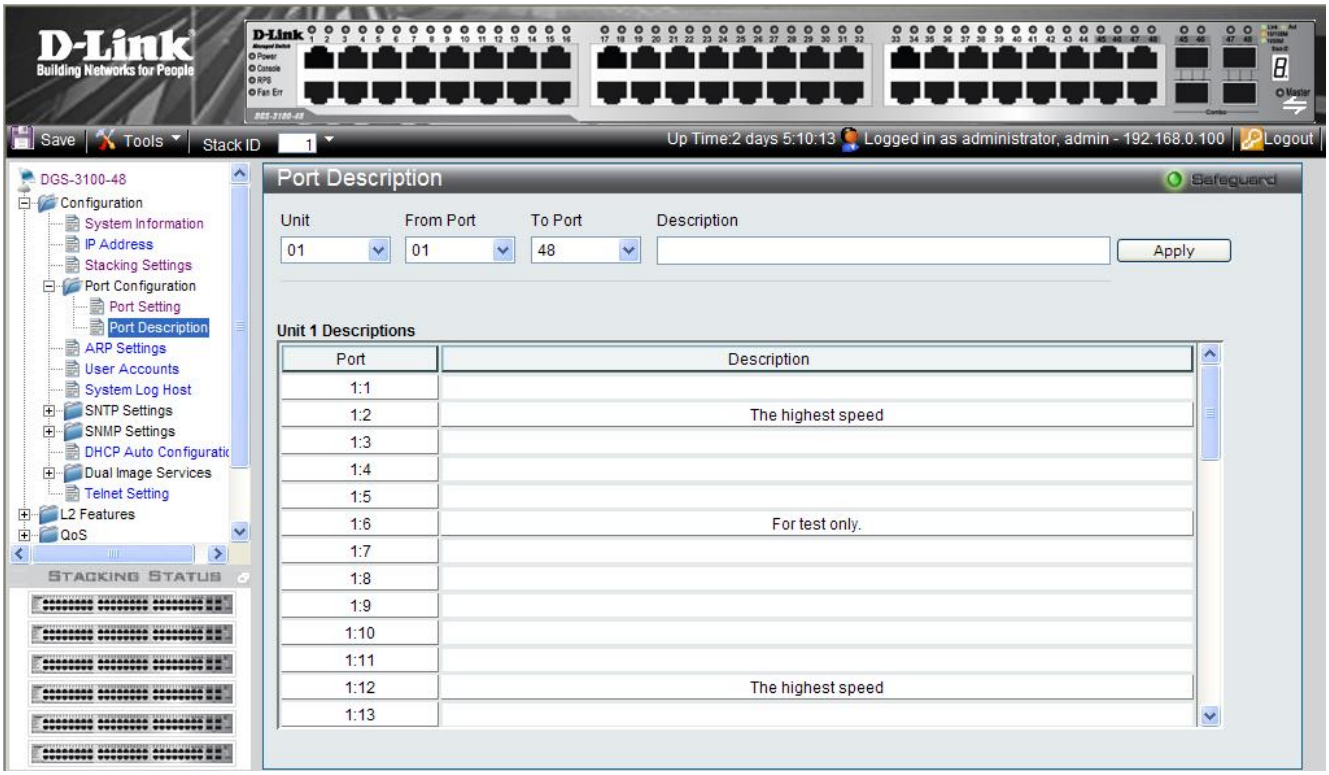


Figure 0-6 Port Description Page

The Port Description Page contains the following fields:

Field	Description
Unit	Defines the stacking member for which the port settings are displayed.
From Port	Defines the port number from which the port parameters are configured.
To Port	Defines the port number to which the port parameters are configured.
Description	Defines a user-defined port description.

2. Define the *Unit*, *From Port*, *To Port*, and *Description* fields.
3. Click Apply. The port description is saved, and the device is updated.

ARP Settings

The *Address Resolution Protocol* (ARP) converts IP addresses into physical addresses and maps the IP address to a MAC address. ARP allows a host to communicate with other hosts only when the IP addresses of its neighbors are known. To define ARP information:

1. Click **Configuration > ARP Settings**. The *ARP Settings Page* opens**:**

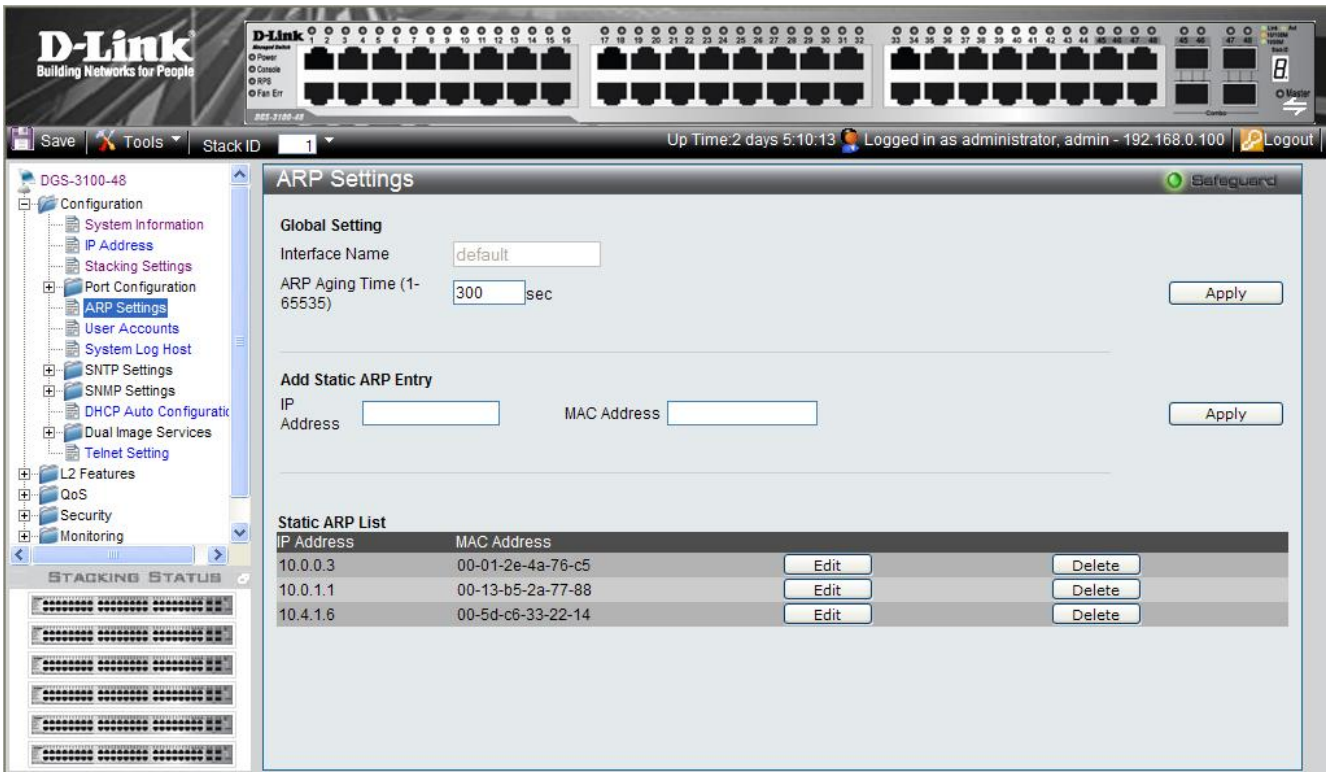


Figure 0-7 ARP Settings Page

The ARP Settings Page contains the following fields:

Field	Description
Interface Name	Defines the interface (VLAN) name.
ARP Aging Time (1-65535)	Defines the amount of time (in seconds) that passes between *ARP Table* entry requests. Following the *ARP Entry Age* period, the entry is deleted from the table. The range is 1 - 65535. The default value is 300 seconds.
IP Address	Defines the station IP address associated with the MAC address.
MAC Address	Defines the station MAC address associated in the ARP table with the IP address.
Static ARP Settings	Displays current static ARP settings table, detailing the user-defined interface name, IP address, and MAC address of each entry.

2. *Define the Interface Name* and *ARP Aging Time* fields.
3. Click Apply. The ARP global setting is updated.
4. Define the *IP Address* and *MAC Address* fields.
5. Click Apply. The ARP settings are saved, and the device is updated**.**

Configuring User Accounts

User accounts including user passwords and access rights are defined on the *User Accounts Page*. To define user account information:

1. Click **Configuration** > **User Account**s. The *User Accounts Page* opens**:**

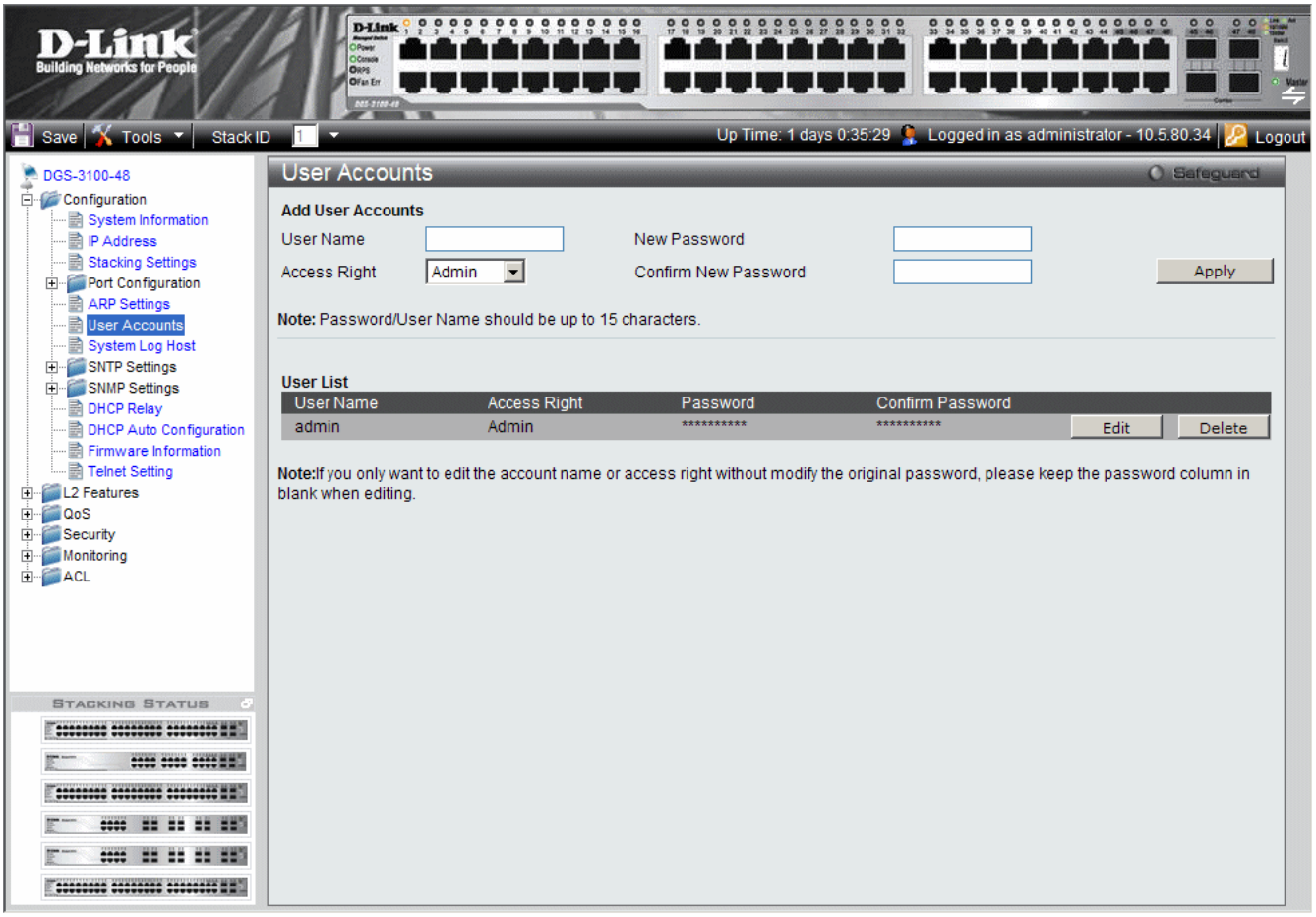


Figure 0-8 User Accounts Page

The User Accounts Page contains the following fields:

Field	Description
User Name	Defines the user name. The user name can contain up-to **15** characters.
New Password	Defines the password assigned to the user account. The password can contain up-to **15** characters.
Access Right	Displays the user access level. The possible field values are: *Admin* — Assigns the user full administrative access through both the Web Interface and the CLI. *Operator* — Assigns the user operator-level access, which is similar to Admin access except that the operator cannot update the firmware, startup configuration, user accounts, or restore factory reset. *User* — Assigns the user read-only access through both the Web Interface and the CLI. The Following limitations appear on the Web Interface: • The 'Save' navigation tree button does not appear and only 'Show Stack Status' feature appears under the 'Tools' button in the Web Interface. • An 'Access Denied' window is displayed, if the user clicks Apply. In order to return to the Web Interface, the user has to go back to the previous page or access a

Field	Description
	different page by using the navigation bar.
Confirm New Password	Confirms the user password.

2. Define the *User Name* field**.**
3. Select the user access level in the *Access Right* field.
4. Enter a new password in the *New Password* field and then re-enter it again in the *Confirm New Password* field.
5. Click Apply. The new user accounts, passwords, and access rights are defined and the device is updated.

NOTE: You are not required to enter a User Name. However, if you do not enter a User Name, you cannot perform the following actions:

- Create a monitor or operator (level 1 or level 14) users until an administrator user (level 15) is defined.
- Delete the last administrator user if there are monitor and/or operator users defined.

To edit the User Accounts Page:

1. Select a name on the *User List*.
2. Click Edit.
3. Define the value.
4. Click Apply. The new access rights are saved, and device is updated.

To delete a User Accounts Page entry:

1. Select an entry.
2. Click Delete. The user account is deleted, and the device is updated.

Managing System Logs

System Logs record and manage events and report errors and informational messages. Event messages have a unique format, as per the Syslog protocols recommended message format for all error reporting. For example, Syslog and local device reporting messages are assigned a severity code, and include a message mnemonic, which identifies the source application generating the message. Messages are filtered based on their urgency or relevancy. Each message severity determines the set of event logging devices that are sent per each event message.

1. Click **Configuration > System Log Host**. The *System Log Host Page* opens**:**

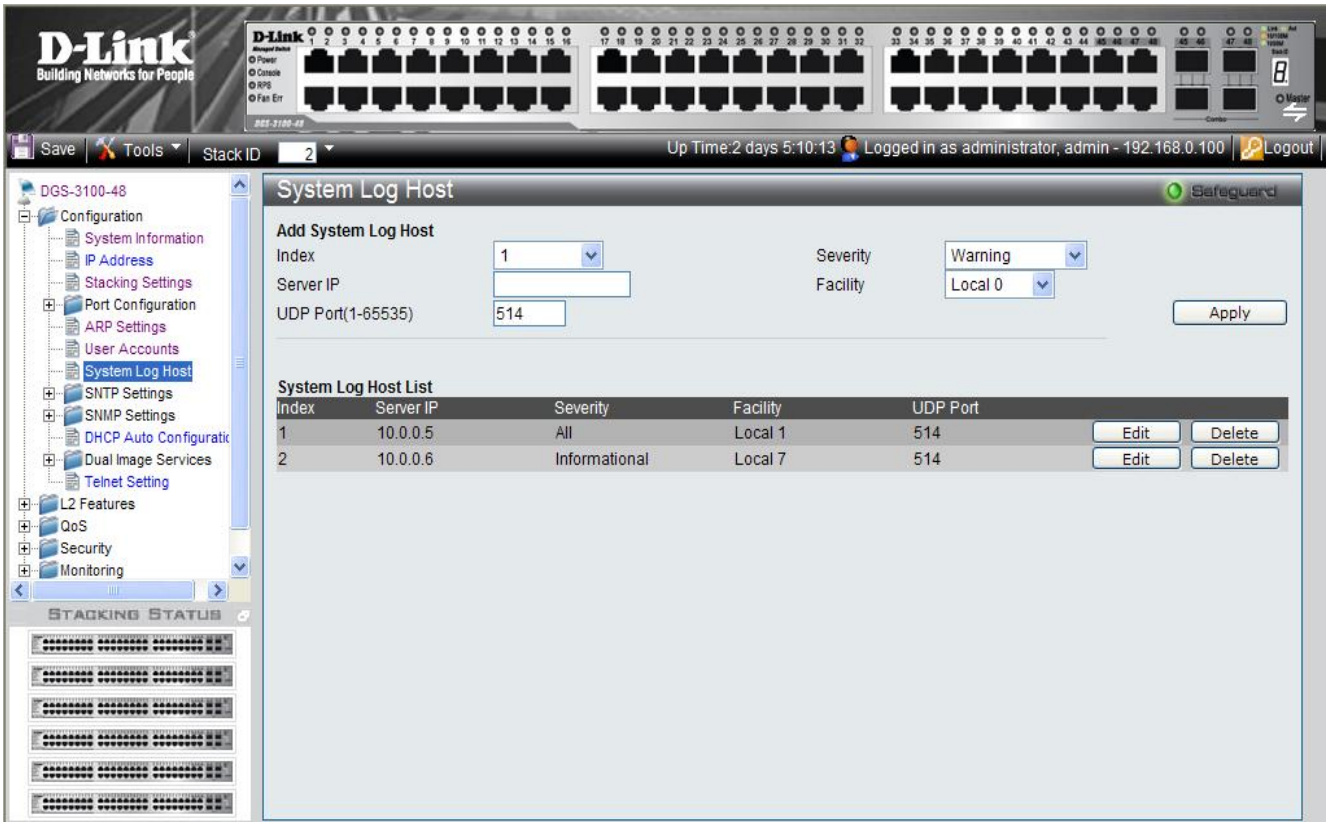


Figure 0-9 System Log Host Page

The System Log Host Page contains the following fields:

Field	Description
Index	Defines syslog host index, 1 out of 4
Severity	Defines the minimum severity from which warning logs are sent to the server. There are two levels. – warning (high) and informational (low): *Warning* —The device is functioning, but an operational problem has occurred. *Informational* — Provides device information through system logs. *All* — Sends system logs for all levels of system logs.
Server IP	Displays the IP address of the Log Server Host.
Facility	Defines an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overridden.
UDP Port(514 or 1-65535)	Defines the UDP port to which the server logs are sent. The possible range is 1 - 65535. The default value is 514.

2. Define the *Index, Severity, Server IP, Facility,* and *UDP Port* fields.
3. Click Apply. The System Log Host is defined, and the device is updated.

To delete a log entry:

4. Select the entry.
5. Click Delete. The entry is deleted, and the device is updated.

Configuring SNTP

The device supports the *Simple Network Time Protocol* (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The device operates only as an SNTP client, and cannot provide time services to other systems. The device polls Unicast type servers for the server time.

Time sources are established by stratums. Stratums define the accuracy of the reference clock. The higher stratum (where zero is the highest), the more accurate clock. The device receives time from stratum 1 and above.

The following is an example of stratums:

Stratum	Example
Stratum 0	A real time clock (such as a GPS system) is used as the time source.
Stratum 1	A server that is directly linked to a Stratum 0 time source is used as the time source. Stratum 1 time servers provide primary network time standards
Stratum 2	The time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server.

Information received from SNTP servers is evaluated based on the Time level and server type. SNTP time definitions are assessed and determined by the following time levels:

Time level	SNTP Time Definition
T1	The time at which the original request was sent by the client.
T2	The time at which the original request was received by the server.
T3	The time at which the server sent the client a reply.
T4	The time at which the client recived the server's reply.

Polling for Time Information

SNTP is used to poll time information from SNTP server. Using SNTP enables accurate system clock.

The *Time Settings Page* allows network managers to enable and configure the SNTP time settings on the device. To enable SNTP:

1. Click **Configuration > SNTP Settings > Time Settings**. The *Time Settings Page* opens**:**

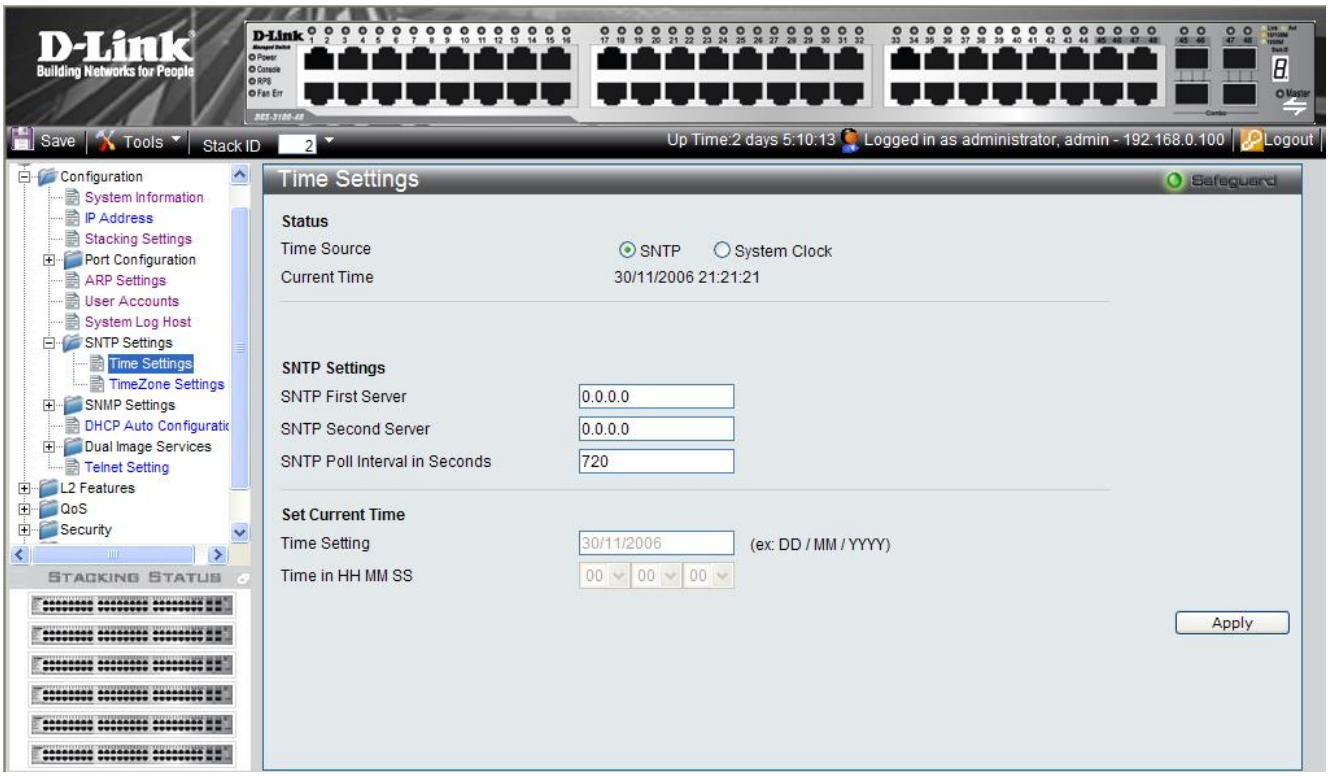


Figure 0-10 Time Settings Page

The Time Settings Page contains the following fields:

Status

Field	Description
Time Source	Defines the time source by which the system time is set. The possible field values are: *SNTP* — Indicates that the system time is retrieved from a SNTP server. *System Clock* — Indicates that the system time is set locally by the device.
Current Time	Displays the current date and time.

SNTP Settings Section

Field	Description
SNTP First Server	Defines the IP address of primary SNTP server from which the system time is retrieved.
SNTP Second Server	Defines the IP address of secondary SNTP server from which the system time is retrieved.
SNTP Poll Interval in Seconds	Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. The range is 60-86400 seconds. The Poll Interval default is 1024 seconds.

Set Current Time

Field	Description
Time Setting	Defines the current system date. The field format is Day/Month/Year.
Time in HH MM SS	Defines the current system time. The field format is HH:MM:SS based on the 24-hour

Field	Description
	clock (Military Time) For example, 9:00PM is configured as 21:00:00.

2. Select a time source in the *Time Source* field.
3. Define the fields.
4. Click Apply. The SNTP settings are defied, and the device is updated.

Configuring Daylight Savings Time

The *TimeZone Settings Page* contains fields for defining system time parameters for both the local hardware clock and the external SNTP clock. If the system time is kept using an external SNTP clock, and the external SNTP clock fails, the system time reverts to the local hardware clock. Daylight saving times can be enabled on the device.

The following is a list of *daylight savings* start and end times in specific countries:

- **Albania** — From the last weekend of March until the last weekend of October.
- **Australia** — From the end of October until the end of March.
- **Australia** - Tasmania — From the beginning of October until the end of March.
- **Armenia** — From the last weekend of March until the last weekend of October.
- **Austria** — From the last weekend of March until the last weekend of October.
- **Bahamas** — From April to October, in conjunction with daylight savings in the United States.
- **Belarus** — From the last weekend of March until the last weekend of October.
- **Belgium** — From the last weekend of March until the last weekend of October.
- **Brazil** — From the third Sunday in October until the third Saturday in March. Clocks go forward one hour in most areas of southeast Brazil for daylight savings.
- **Chile** —Easter Island: from March 9 until October 12. The rest of the country, from the first Sunday in March, or after March 9.
- **China** — China does not use daylight saving time.
- **Canada** — From the first Sunday in April until the last Sunday of October. Daylight saving times are usually regulated by provincial and territorial governments. Exceptions may exist in certain municipalities.
- **Cuba** — From the last Sunday of March to the last Sunday of October.
- **Cyprus** — From the last weekend of March until the last weekend of October.
- **Denmark** — From the last weekend of March until the last weekend of October.
- **Egypt** — From the last Friday in April until the last Thursday in September.
- **Estonia** — From the last weekend of March until the last weekend of October.
- **Finland** — From the last weekend of March until the last weekend of October.
- **France** — From the last weekend of March until the last weekend of October.
- **Germany** — From the last weekend of March until the last weekend of October.
- **Greece** — From the last weekend of March until the last weekend of October.
- **Hungary** — From the last weekend of March until the last weekend of October.
- **India** — India does not use daylight saving time.
- **Iran** — From Farvardin 1 until Mehr 1.
- **Iraq** — From April 1 until October 1.
- **Ireland** — From the last weekend of March until the last weekend of October.
- **Israel** — Varies year-to-year.
- **Italy** — From the last weekend of March until the last weekend of October.
- **Japan** — Japan does not use daylight saving time.
- **Jordan** — From the last weekend of March until the last weekend of October.
- **Latvia** — From the last weekend of March until the last weekend of October.
- **Lebanon** — From the last weekend of March until the last weekend of October.

- **Lithuania** — From the last weekend of March until the last weekend of October.
- **Luxembourg** — From the last weekend of March until the last weekend of October.
- **Macedonia** — From the last weekend of March until the last weekend of October.
- **Mexico** — From the first Sunday in April at 02:00 to the last Sunday in October at 02:00.
- **Moldova** — From the last weekend of March until the last weekend of October.
- **Montenegro** — From the last weekend of March until the last weekend of October.
- **Netherlands** — From the last weekend of March until the last weekend of October.
- **New Zealand** — From the first Sunday in October until the first Sunday on or after March 15.
- **Norway** — From the last weekend of March until the last weekend of October.
- **Paraguay** — From April 6 until September 7.
- **Poland** — From the last weekend of March until the last weekend of October.
- **Portugal** — From the last weekend of March until the last weekend of October.
- **Romania** — From the last weekend of March until the last weekend of October.
- **Russia** — From the last weekend of March until the last weekend of October.
- **Serbia** — From the last weekend of March until the last weekend of October.
- **Slovak Republic** - From the last weekend of March until the last weekend of October.
- **South Africa** — South Africa does not use daylight saving time.
- **Spain** — From the last weekend of March until the last weekend of October.
- **Sweden** — From the last weekend of March until the last weekend of October.
- **Switzerland** — From the last weekend of March until the last weekend of October.
- **Syria** — From March 31 until October 30.
- **Taiwan** — Taiwan does not use daylight saving time.
- **Turkey** — From the last weekend of March until the last weekend of October.
- **United Kingdom** — From the last weekend of March until the last weekend of October.
- **United States of America** — From the second Sunday in March at 02:00 to the first Sunday in November at 02:00.

To configure the system time:

- Click **Configuration > SNTP Settings > TimeZone Settings**. The *TimeZone Settings Page* opens**:**

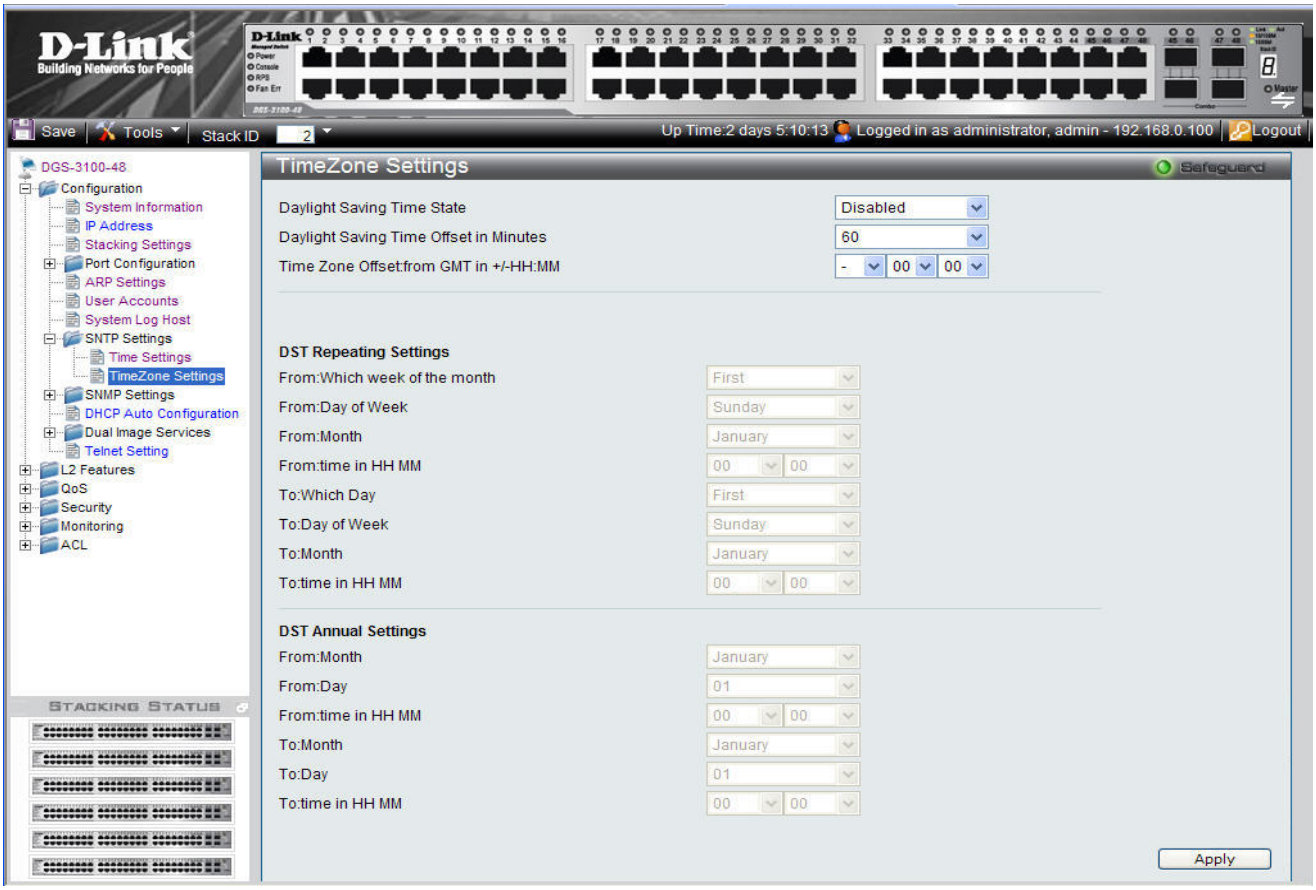


Figure 0-11 TimeZone Settings Page

The TimeZone Settings Page contains the following fields:

Field	Description
Daylight Savings Time State	Defines type of DST enabled on the device. The possible field values are: Disable — Disables DST on the device. This is the default values. Repeating — Enables setting repeating DST. This option requires defining begin and end times by specific date and hour. Annual — Enables setting annual DST. This option requires defining begin and end times by the specific dates.
Daylight Saving Time Offset in Minutes	Defines the local DST offset in minutes. The default time is 60 minutes. The possible field values are: 30 — Defines the local offset for 30 minutes. 60 — Defines the local offset for 60 minutes. 90 — Defines the local offset for 90 minutes. 120 — Defines the local offset for 120 minutes.
Time Zone Offset:from GMT	Indicates the difference between *Greenwich Mean Time* (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1, while the Time Zone Offset for New York is GMT –5.

DST Repeating Settings Sections

The *Repeating Mode* enables setting repeating DST. This option requires defining begin and end times by specific day and hour. For example, the network administrator defines that DST begins the second Saturday during April and ends on the last Sunday in October.

Field	Description

Field	Description
From Which Week of the Month	Defines which numeric week of the month DST begins. The possible field values are: *First* — Indicates the first week of a month. *Second* — Indicates the second week of a month. *Third* — Indicates the third week of a month. *Fourth* — Indicates the fourth week of a month.
From Day of Week	Defines the week day DST starts. The field range is Sunday–Saturday.
From Month	Defines the month DST starts. The field range is January–December.
From time in HH MM	Defines the time of day DST starts. The field format is Hour:Minutes based on the 24-hour clock (Military Time). For example, 9:00PM is configured as 21:00.
To Which Week of the Month	Defines which numeric week of the month DST ends. The possible field values are: *First* — Indicates the first week of a month. *Second* — Indicates the second week of a month. *Third* — Indicates the third week of a month. *Fourth* — Indicates the fourth week of a month.
To Day of Week	Defines the week day DST ends. The field range is Sunday–Saturday.
To Month	Defines the month DST ends. The field range is January–December.
To time in HH MM	Defines the time of day DST ends. The field format is Hour:Minutes based on the 24-hour clock (Military Time). For example, 9:00PM is configured as 21:00.

DST Annual Settings Section

The *Annual Mode* enables setting a DST seasonal time adjustment. This option requires defining *begin* and *end* times by the specific dates. For example, the network administrator defines that DST begins April 3 and ends October 14.

Field	Description
From:Month	Defines the month of the year that DST starts. The field options are January-December.
From:Day	Defines the date on which DST starts. The field options are 1-31.
From:Time	Defines the time at which DST starts. The field format is HH:MM based on the 24-hour clock (Military Time) For example, 9:00PM is configured as 21:00.
To:Month	Defines the month of the year in which DST ends. The field options are January-December.
To:Day	Defines the date on which DST ends. The field options are 1-31.
To:Time	Defines the time at which DST ends. The field format is HH:MM based on the 24-hour clock (Military Time) For example, 9:00PM is configured as 21:00.

1. Select a daylight savings time source in the *Daylight Saving Time State* field.
2. Define the fields.
3. Click Apply. Daylight Savings Time is configured, and the device is updated.

Configuring SNMP

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports the following SNMP versions:

- SNMP version 1
- SNMP version 2c
- SNMP version 3

SNMP v1 and v2c

The SNMP agents maintain a list of variables used to manage the device. The variables are defined in the *Management Information Base* (MIB). The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agents are controlled by access strings.

SNMP v3

SNMP v3 applies access control and a new traps mechanism. In addition, *User Security Model* (USM) parameters are defined for SNMPv3, including:

Parameters	Description
Authentication	Provides data integrity and data origin authentication.
Privacy	Prevents message content disclosure. *Cipher Block-Chaining* (CBC) is used for encryption. Either authentication is enabled on a SNMP message, or both authentication and privacy are enabled on an SNMP message. However, privacy cannot be enabled without authentication.
Key Management	Defines key generation, key updates, and key use.

The device supports SNMP notification filters based on *Object IDs* (OIDs). OIDs are used by the system to manage device features.

SNMP v3 supports the following features:

- Security
- Feature Access Control
- Traps

The system comes up with SNMP disabled. The following communities are defined by default:

- PRIVATE: Read/write community
- PUBLIC: Read only community

The user cannot connect through an NMS application without enabling the SNMP service.

Defining SNMP Settings

You can globally enable or disable SNMP in the SNMP Global Settings Page.

1. Click **Configuration > SNMP Settings > SNMP Global Settings**. The SNMP Global Settings Page opens:

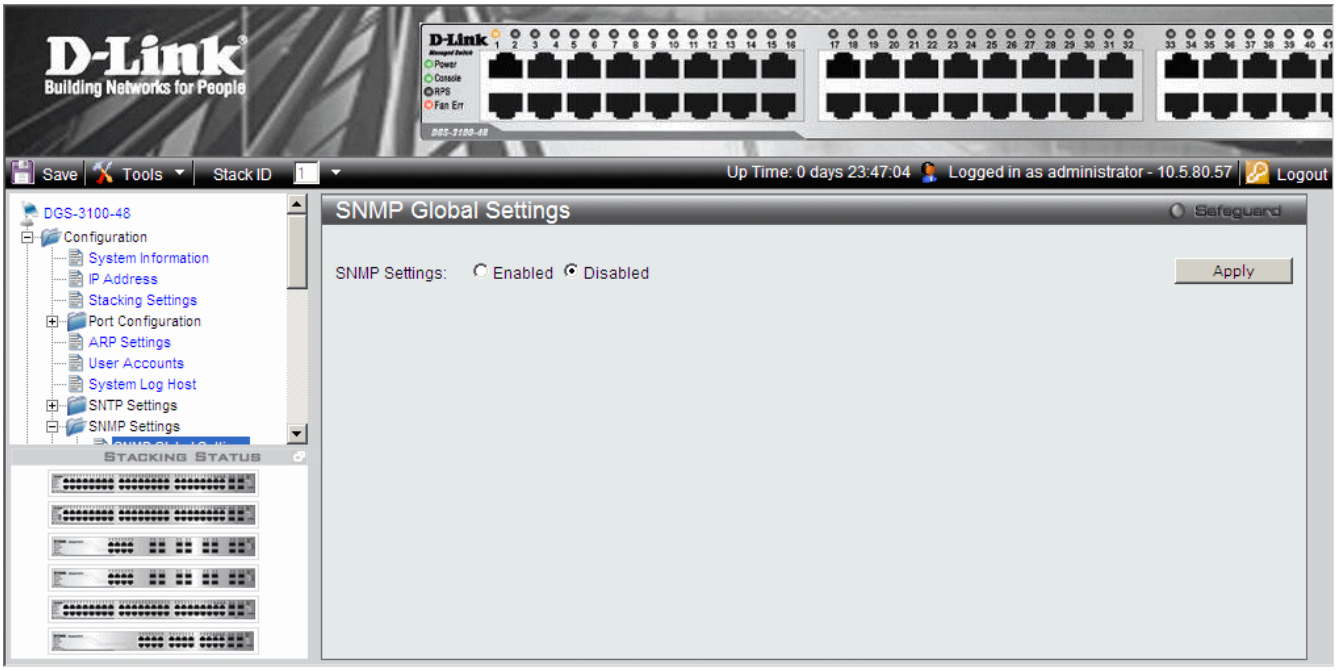


Figure 0-12 SNMP Global Settings Page

2. Select either Enabled or Disabled to enable/disable SNMP.
3. Click Apply. The SNMP is enabled.

•

Defining SNMP Views

SNMP views provide or block access to device features or aspects of features. For example, a view can be defined to show that SNMP view A has *included* access to Multicast groups, while SNMP view B has *excluded* access to Multicast groups. Feature access is granted via the MIB name or MIB Object ID.

1. Click **Configuration > SNMP Settings > SNMP View Table**. The *SNMP View Table Page* opens**:**

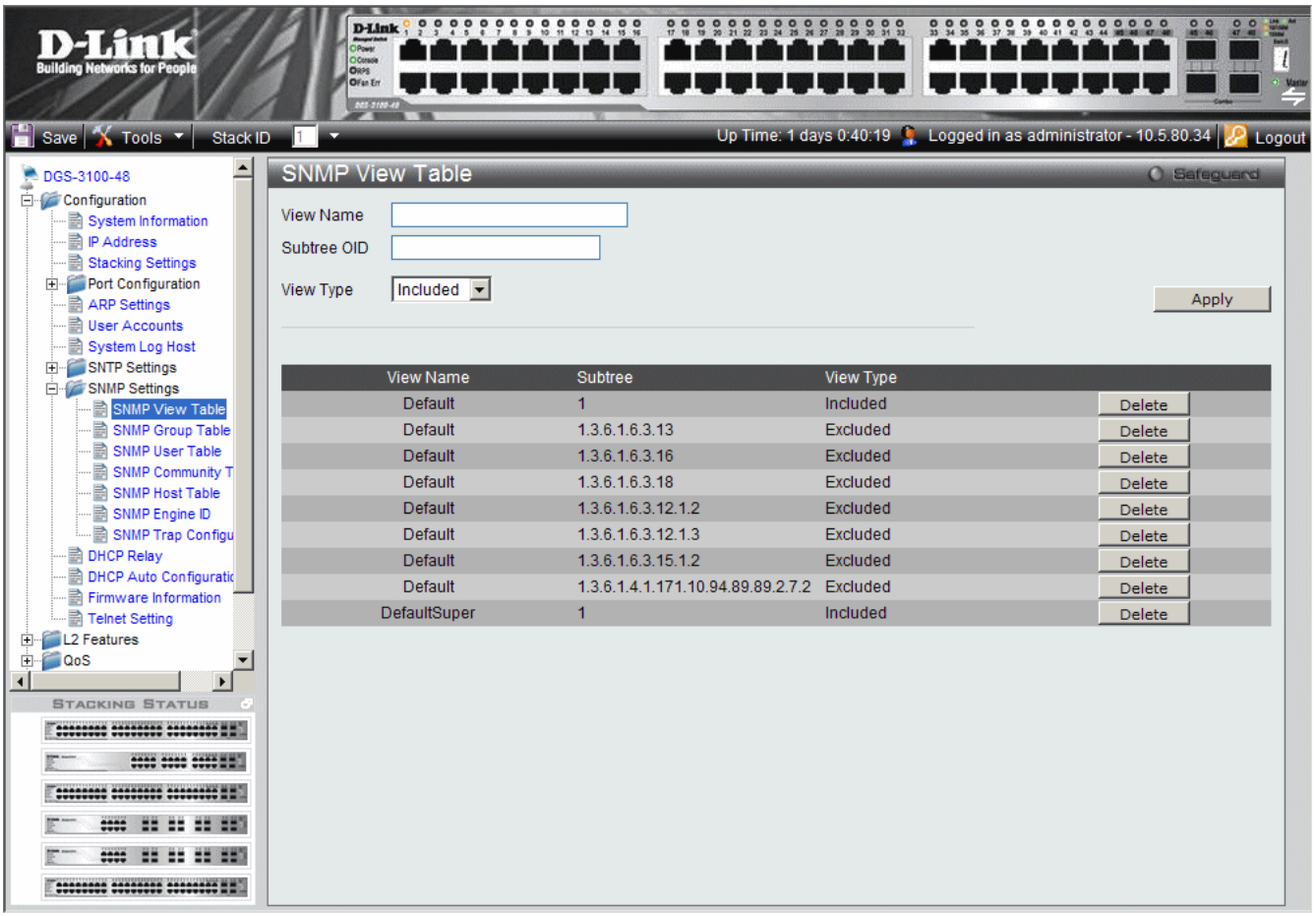


Figure 0-13 SNMP View Table Page

The SNMP View Table Page contains the following fields:

Field	Description
View Name	Defines the *view* name (limited to 30 alphanumeric characters).
Subtree OID	Defines the OID included in, or excluded from, the selected SNMP view.
View Type	Defines whether the defined OID branch will be included in, or excluded from, the selected SNMP view.

2. Define the *View Name*, *Subtree OID* and *View Type* fields.
3. Click Apply. The SNMP View Table is defined, and the device is updated.

To delete a view from the SNMP View Table Page:

4. Select an entry on the list.
5. Click Delete. The entry is deleted, and the device is updated.

Defining SNMP Groups

The *SNMP Group Table Page* provides information for creating SNMP groups and assigning SNMP access control privileges to SNMP groups. Groups enable network managers to assign access rights to specific device features or feature aspects. To define SNMP groups:

1. Click **Configuration > SNMP Settings > SNMP Group Table**. The *SNMP Group Table Page* opens**:**

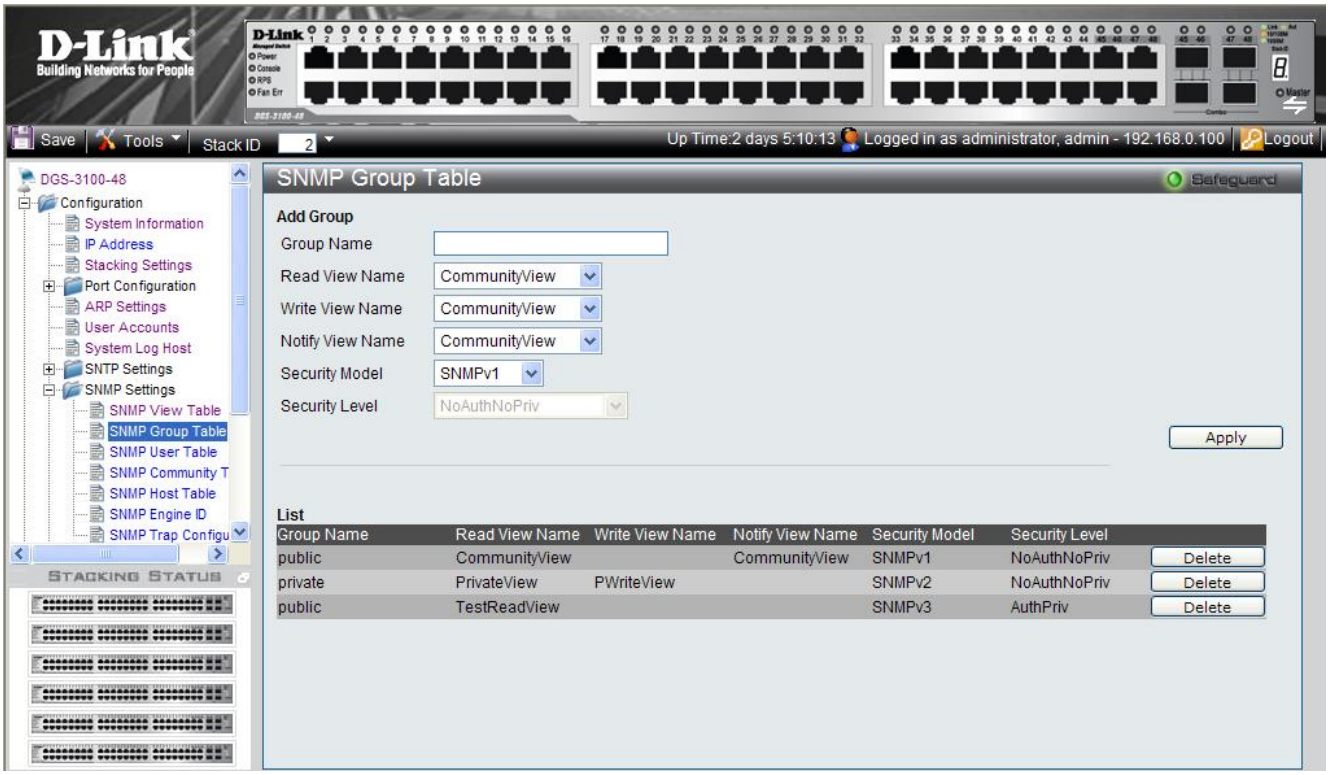


Figure 0-13 SNMP Group Table Page

The SNMP Group Table Page contains the following fields:

Field	Description
Group Name	Defines the user-defined group name to which access control rules are applied (limited to 30 alphanumeric characters).
Read View Name	Defines a Read Only view. The Read Only view management access is restricted to read-only, and changes cannot be made to the assigned SNMP view. The possible values are: *Community/View* *TestReadView* *PWriteView* *PrivateView*
Write View Name	Defines a Write view. The Management view access is read/write, and changes can be made to the assigned SNMP view. The possible values are: *Community/View* *TestReadView* *PWriteView* *PrivateView*

Field	Description
Notify View Name	Defines a Notify view. The Notify view sends traps for the assigned SNMP view. This is applicable for SNMPv3 only. The possible values are: *Community/View* *TestReadView* *PWriteView* *PrivateView*
Security Model	Defines the SNMP version attached to the group. The possible field values are: *SNMPv1* — Defines SNMPv1 as the security model for the group. *SNMPv2* — Defines SNMPv2 as the security model for the group. *SNMPv3* — Defines SNMPv3 as the security model for the group.
Security Level	Defines the security level attached to the group. Security levels apply to SNMPv3 only. The possible field values are: *NoAuthNoPriv* — Defines that neither the Authentication nor the Privacy security levels are assigned to the group. *AuthNoPriv* — Authenticates SNMP messages, and ensures that the SNMP message's origin is authenticated. *AuthPriv* — Encrypts SNMP messages.

2. Define the *Group Name*, *Read View Name*, *Write View Name*, and *Notify View Name* fields.
3. Select a security model from the *Security Model* list.
4. Click Apply. The SNMP groups are defined, and the device is updated.

To delete a Group Name from the SNMP Group Table Page List:

5. Select a Group Name.
6. Click Delete. The Group Name is deleted, and the device is updated.

Defining SNMP Users

The *SNMP User Table Page* enables assigning system users to SNMP groups and defining the user authentication method. To assign system users:

1. Click **Configuration > SNMP Settings >SNMP User Table**. The *SNMP User Table Page* opens:

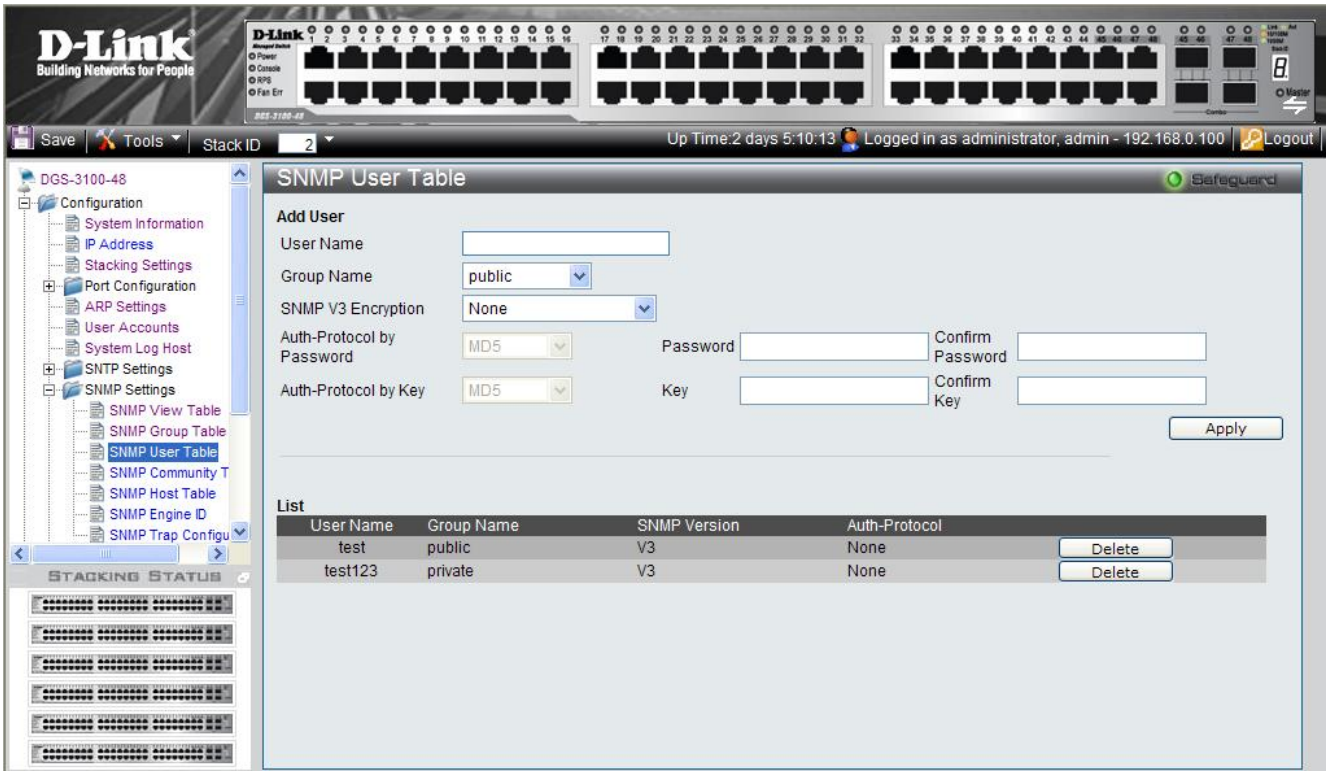


Figure 0-145 SNMP User Table Page

The SNMP User Table Page contains the following fields:

Field	Description
User Name	Defines the SNMP user name included in the SNMP user group.
Group Name	Defines the SNMP group and assigned to a user.
SNMP V3 Encryption	Defines the SNMPv3 user authentication method. The possible field values are: *None* —No user authentication is used. *Password* — Provides user authentication via the HMAC-SHA-96 authentication level password or HMAC-MD5-96 password. *Key* — Provides user authentication via the HMAC-MD5 algorithm or the HMAC-SHA-96 authentication level.
Auth-Protocol by Password	Selects the authentication password type used to authenticate users. The possible field values are: *MD5* — Defines that HMAC-MD5-96 password is used for authentication. *SHA* — Defines that HMAC-SHA-96 authentication level password is used for authentication.
Password	Defines the password used for authentication. (1-32 digits).
Confirm Password	Confirms the password used for authentication. (1-32 digits).

Field	Description
Auth-Protocol by Key	Selects the authentication key type used to authenticate users. The possible field values are: *MD5* — Defines that users are authenticated via a HMAC-MD5 algorithm key. *SHA* — Defines that users are authenticated via a HMAC-SHA-96 authentication level key.
Key	Defines the authentication key for authentication (MD5 – 32 or 64 digits), (SHA – 40 or 70 digits).
Confirm Key	Confirms the authentication key for authentication.

2. Define the *User Name*, *Group Name*, and *SNMP V3 Encryption* fields.
3. Define the authentication password or authentication key.
4. Click Apply. The SNMP authentication method is defined, and the device is updated.

Defining SNMP Communities

Access rights are managed by defining communities, using the *16 SNMP Community Table* Page. When the community names are changed, access rights are also changed. SNMP communities are defined only for SNMP v1 and SNMP v2c. To define SNMP communities:

1. Click **Configuration > SNMP Settings > SNMP Community Table**. The *16 SNMP Community Table* **Page** opens**:**

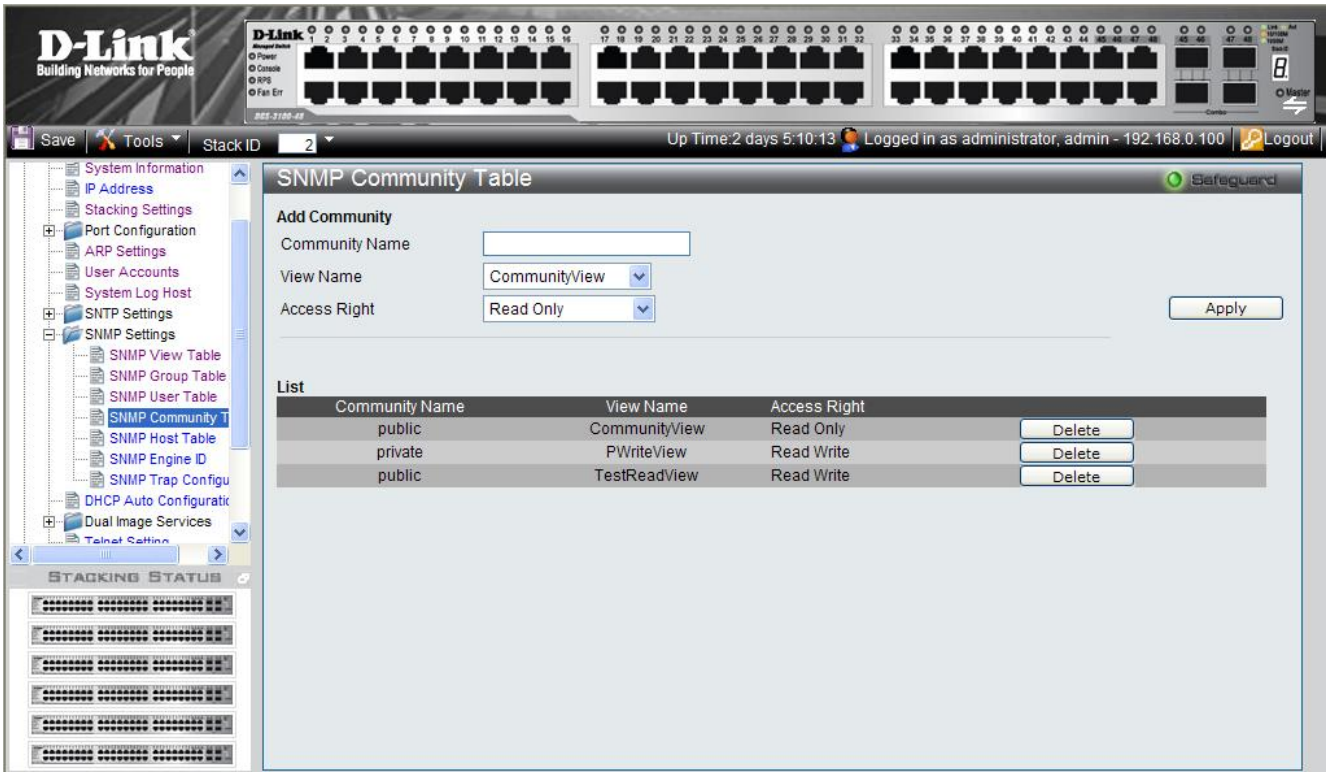


Figure 0-16 SNMP Community Table Page

The 16 SNMP Community Table Page contains the following fields:

Field	Description
Community Name	Defines advanced SNMP community name (limited to 20 alphanumeric characters).
View Name	Defines the group of MIB objects that a remote SNMP manager is allowed to access on the switch.
Access Rights	Defines the access rights of the community. The possible field values are: *Read Only* — Management access is restricted to read only, and changes cannot be made to the community. *Read Write* — Management access is read/write and changes can be made to the device configuration, but not to the community.

2. Define the Community Name, and View Name, Access Right fields.
3. Click Apply. The SNMP Community Table is defined, and the device is updated.

To delete a 16 SNMP Community Table Page List entry:

1. Select a Community Name.
2. Click Delete. The entry is deleted, and the device is updated**.**

Defining SNMP Host Table

The *SNMP Host Table Page* contains information for defining filters that determine whether traps are sent to specific host, as well as the trap type sent.

To define the SNMP Host Table Page:

1. Click **Configuration > SNMP Settings > SNMP Host Table**. The *SNMP Host Table Page* opens:

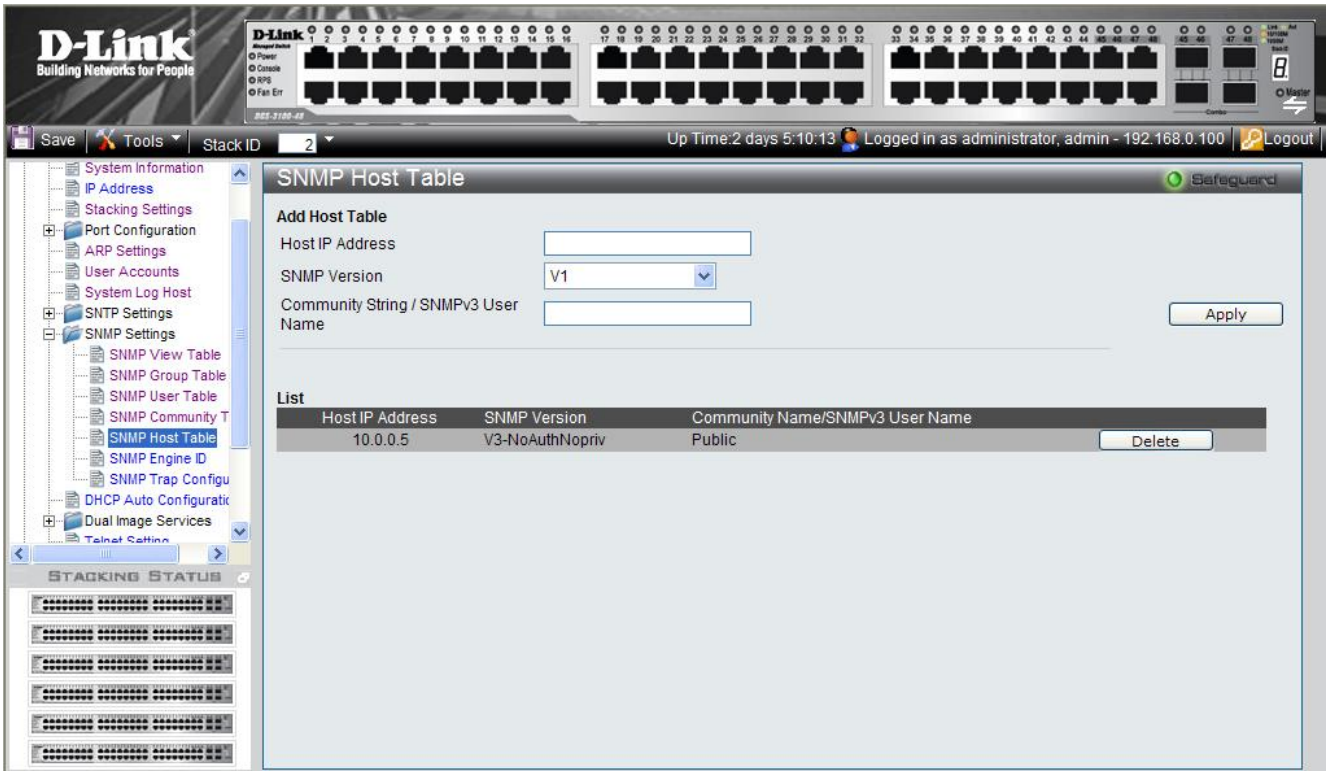


Figure 0-17 SNMP Host Table Page

The SNMP Host Table Page contains the following fields:

Field	Description
Host IP Address	Defines the IP address to which the traps are sent.
SNMP Version	Defines the trap type. The possible field values are: *SNMPV1* — Indicates that SNMP Version 1 traps are sent. *SNMPV2c* —Indicates that SNMP Version 2 traps are sent. *SNMPV3-NoAuth-NoPriv* — Indicates that the SNMP version 3 is assigned with a NoAuth-NoPriv security level and traps of that level will be sent *SNMPV3-Auth-NoPriv* — Indicates that the SNMP version 3 is assigned with an Auth-NoPriv security level and traps of that level will be sent *SNMPV3-Auth-Priv* — Indicates that the SNMP version 3 is assigned with an Auth-Priv security level and traps of that level will be sent
Community String / SNMPv3 User Name	Defines the community string or assigned to the SNMP V3 user.

2. Define the Host IP Address field.
3. Select the trap type in the SNMP Version field.
4. Define the Community String / SNMPv3 User Name field.
5. Click Apply. The SNMP Host Table is defined, and the device is updated.

To delete a SNMP Host Table Page List entry:

1. Select an entry.
2. Click Delete. The entry is deleted, and the device is updated.

Defining SNMP Engine ID

The Engine ID is a unique identifier used for SNMP V3 implementations. This is an alphanumeric string used to identify the SNMP engine on the switch. To define the SNMP Engine ID:

1. Click **Configuration > SNMP Settings > SNMP Engine ID**. The *SNMP Engine ID Page* opens:

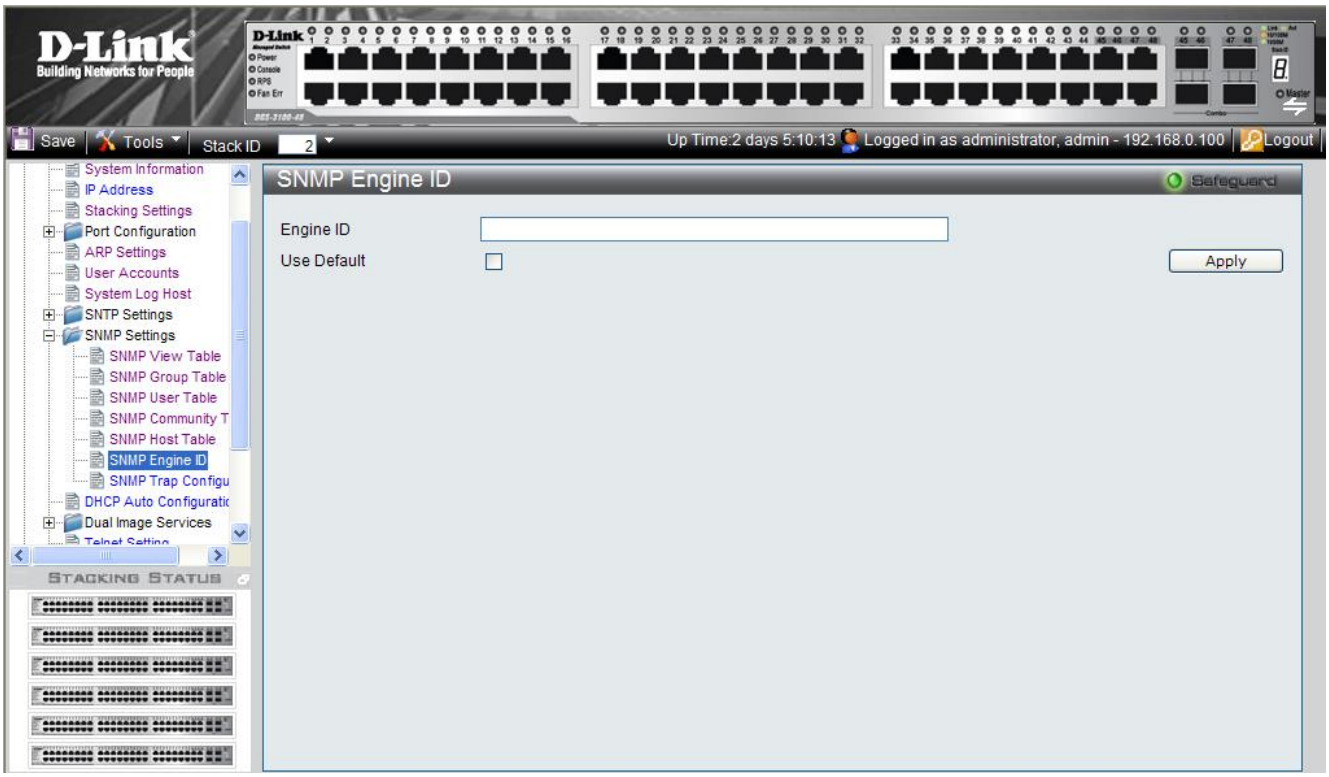


Figure 0-18 SNMP Engine ID Page

The SNMP Engine ID Page contains the following fields:

Field	Description
Engine ID	Defines the local device Engine ID. The field value is a hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon. The Engine ID must be defined before SNMPv3 is enabled. Select a default Engine ID that is comprised of an Enterprise number and the default MAC address.
Use Default	When selected, provides the device-generated Engine ID. The default Engine ID is based on the device MAC address and is defined per standard as: *First 4 octets* — first bit = 1, the rest is IANA Enterprise number. *Fifth octet* — Set to 3 to indicate the MAC address that follows. *Last 6 octets* — MAC address of the device.

2. Define the *Engine ID* or *Use Default* checkbox.
3. Click Apply. The SNMP Engine ID is defined, and the device is updated.

Enabling SNMP Traps

The *SNMP Configuration Trap Page* contains parameters for defining SNMP notification parameters. To enable SNMP notifications: To enable SNMP Traps:

1. Click **Configuration > SNMP Settings > SNMP Trap Configuration.** The *SNMP Configuration Trap Page* opens**:**

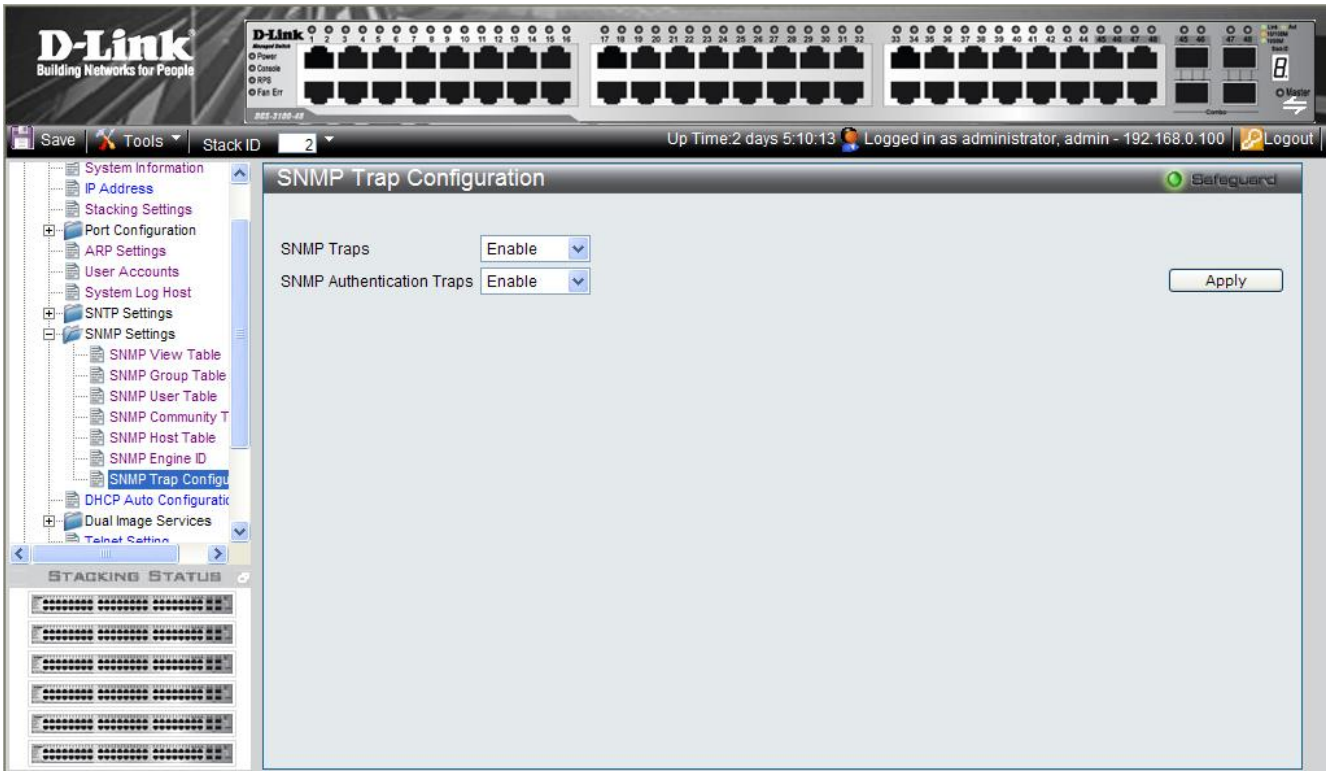


Figure 0-19 SNMP Configuration Trap Page

The SNMP Configuration Trap Page contains the following fields:

Field	Description
SNMP Traps	Specifies whether the device can send SNMP notifications. The possible field values are: *Enable* — Enables SNMP notifications. This is the default value. *Disable* — Disables SNMP notifications.
SNMP Authentication Traps	Specifies whether the device can send traps upon *authentication failure* notification. *Enable* — Enables the device to send authentication failure notifications. This is the default value. *Disable* — Disables the device from sending authentication failure notifications.

2. Define the SNMP Traps and SNMP Authentication Traps fields.
3. Click Apply. The SNMP trap status is modified, and the device is updated.

DHCP Relay

The *DHCP Relay Page* allows the user to enable DHCP relay and define DHCP relay servers on the device.

The Relay agent information option known as Option 82 is part of the DHCP protocol and allows a DHCP relay agent to send additional client information upon requesting an IP address. A DHCP relay agent detects DHCP broadcasts from DHCP clients and relays those broadcasts to DHCP servers on different subnets.

In addition, when client ingress VLAN information differs from the VLAN on which DHCP servers are connected, Option 82 information is added to the packets relayed to DHCP server. Option 82 specifies the relaying switch's MAC address, the port identifier, and specifies the VLAN forwarding the packet.

To define **DHCP Relay Server** Information:

1. Click **Configuration** > **DHCP Relay**. The *DHCP Relay Page* opens**:**

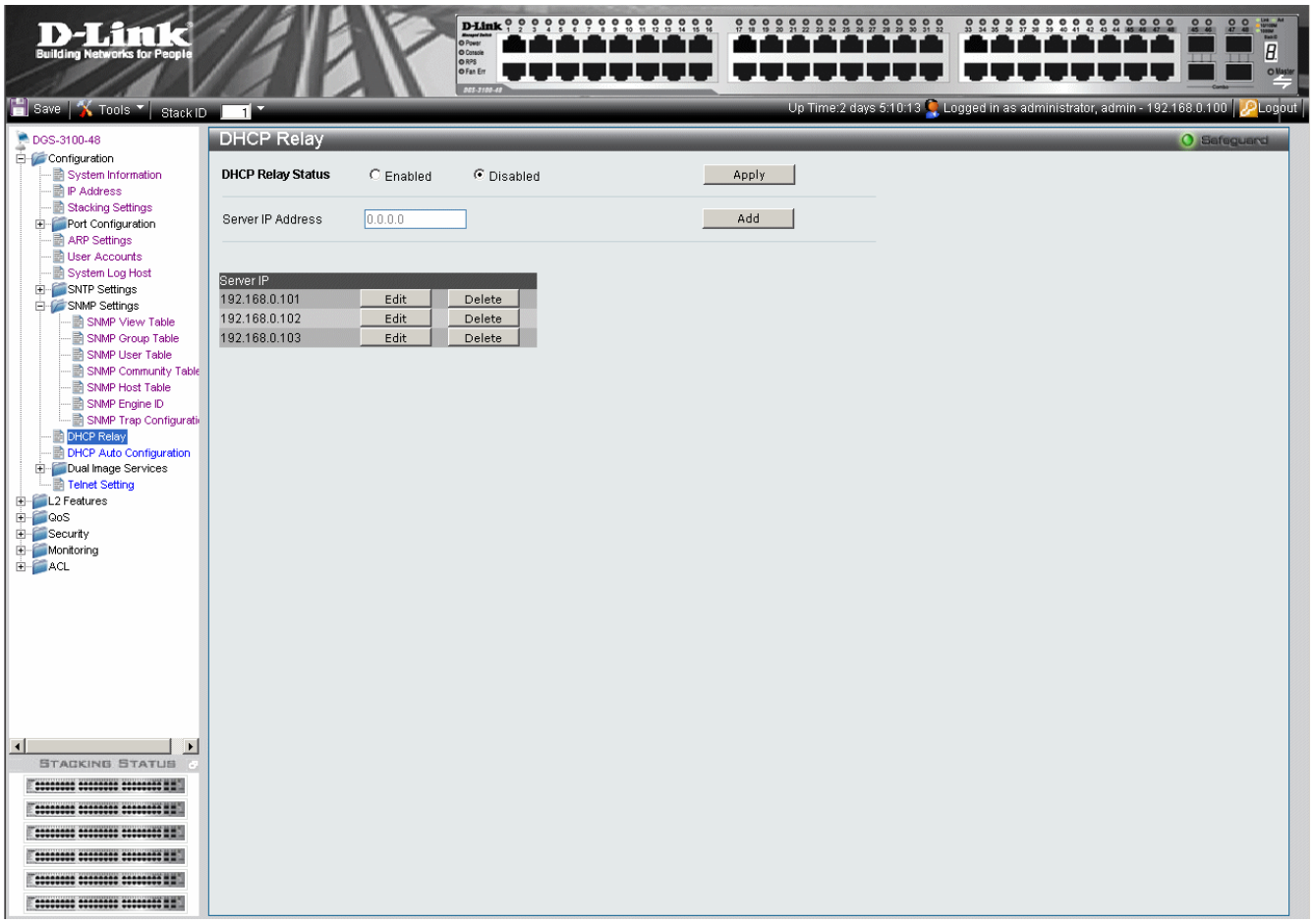


Figure 0-20 DHCP Relay Page

The DHCP Relay Page contains the following fields:

Field	Description
DHCP Relay Status	Specifies whether the DHCP is enabled on the device. The possible field values are: • *Enabled* — Enables DHCP Relay on the device. • *Disabled* — Disables DHCP Relay on the device. This is the default value.
Server IP Address	Defines the DHCP relay server's IP address
Server IP	Display the list of user-defined DHCP Relay servers.

2. Select Enabled to enable DHCP Relay. Disabled is the default.
3. Click Apply. The DHCP Relay servers are defined, and the device is updated**.**

DHCP Local Relay

The *DHCP Local Relay Page* allows the user to configure DHCP Local Relay. This is done by enabling the DHCP Local Relay feature.

Requests

- DHCP broadcasts are trapped by the switch CPU, and replacement broadcasts are forwarded with Option 82.

Replies from the DHCP servers are trapped by the switch CPU, the Option 82 is removed and the reply is sent to the DHCP Client.

To define DHCP Local Relay Server Information:

1. Click **Configuration > DHCP Local Relay**. The *DHCP Relay Page* opens**:**

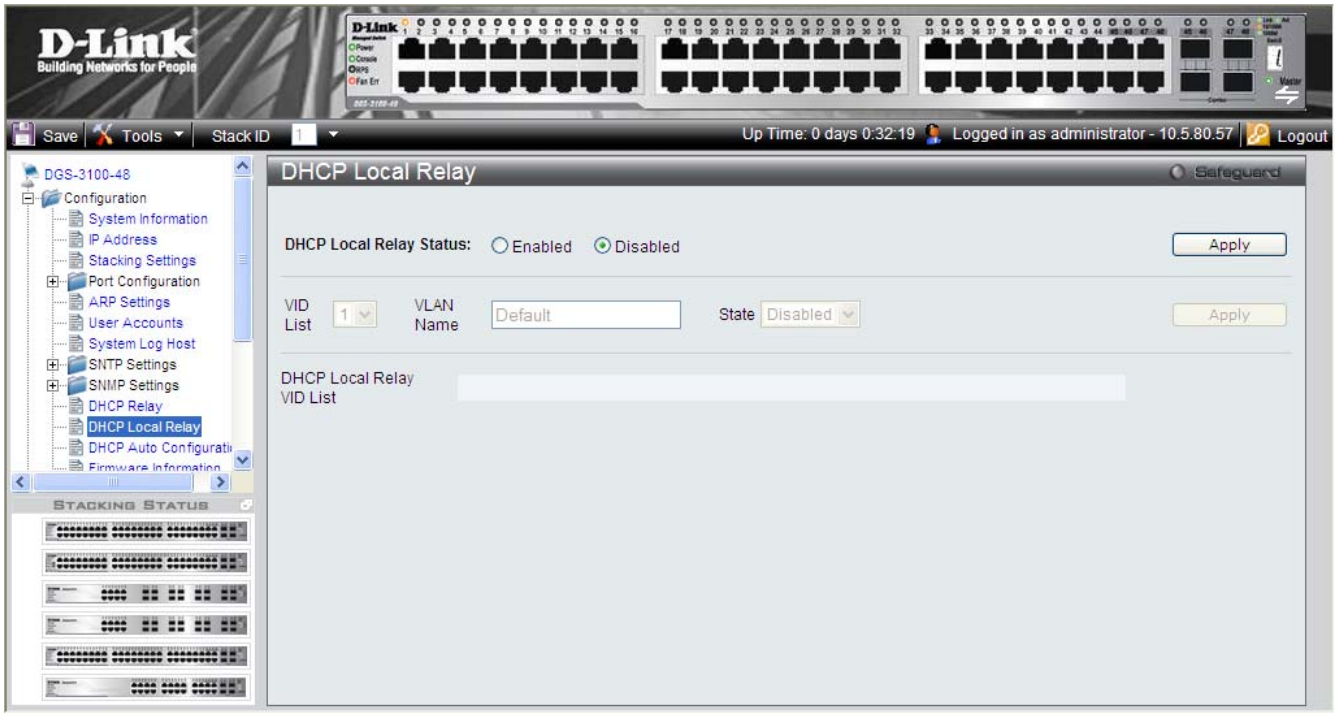


Figure 0-15 DHCP Local Relay Page

The DHCP Relay Page contains the following fields:

Field	Description
DHCP Local Relay Status	Specifies whether DHCP Local Relay is enabled on the device. The possible field values are: • *Enabled* — Enables DHCP Local Relay on the device. • *Disabled* — Disables DHCP Local Relay on the device. This is the default value.
VID List	Specifies on which VLAN DHCP Local Relay is enabled.
VLAN Name	Displays the name of the selected VLAN.
State	Specifies whether DHCP Local Relay is enabled on the VLAN. The possible field values are: • *Enabled* — Enables DHCP Local Relay on the VLAN. • *Disabled* — Disables DHCP Local Relay on the VLAN. This is the default value.
DHCP Local Relay VID List	Displays the list of VLANs on which DHCP Local Relay has been defined

2. Select Enabled to enable DHCP Relay on the device.
3. Click the upper Apply. The DHCP Local Relay feature is activated, and the device is updated.
4. Select a VLAN on which DHCP Local Relay is to be activated.

5. Click Apply. DHCP Local Relay is defined on the selected VLAN and it is displayed in the DHCP Local Relay VID List.
6. Repeat steps 4 and 5 for all required VLANs.

.

DHCP Auto Configuration

In the DHCP Auto Configuration Page, users can enable or disable automatic download of the latest image and configuration files from the DHCP server. During reboot, if DHCP Auto Configuration is enabled, the device polls the TFTP Server. From the DHCP server, the device receives the following, if necessary:

- **IP address** – The device will receive IP from the DHCP server regardless of current IP configuration (whether static or dynamic). If the device already has a DHCP-defined IP address, it will retain the current address. If Static IP is present in the configuration file, it will be ignored.
- **Image file** – If an updated image file is available on the network, and the DHCP server's latest instruction file refers to it, the device downloads the image file.
- **Configuration file** – If an updated configuration file is available on the network, and the DHCP server's latest instruction file refers to it, the device downloads the file as its new Running Configuration, and also saves it as the Startup Configuration. If Static IP is present in the configuration file, it will be ignored.

To enable DHCP Auto Configuration:

1. Click **Configuration > DHCP Auto Configuration**. The *DHCP Auto Configuration Page* opens:

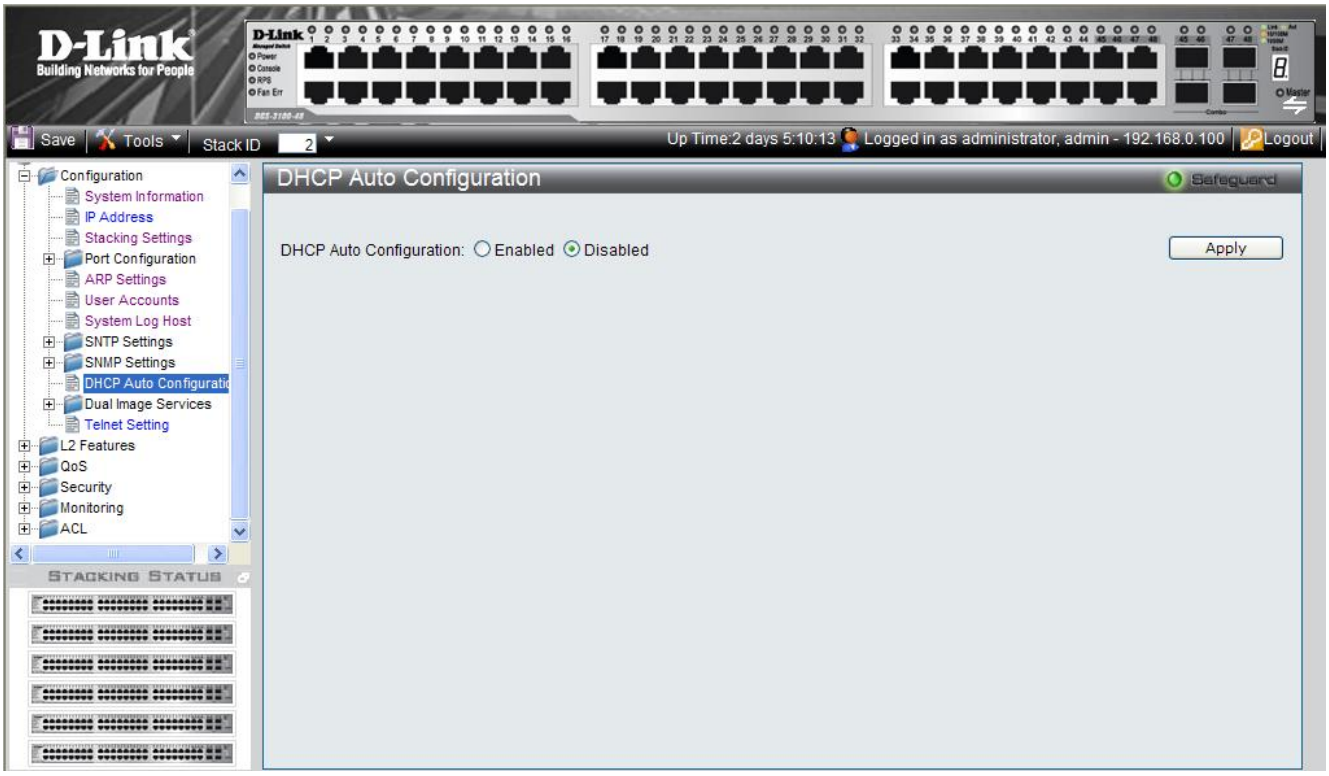


Figure 0-22 DHCP Auto Configuration Page

The DHCP Auto Configuration Page contains the following fields:

Field	Description
DHCP Auto Configuration	Specifies whether the device gets an updated image file, and updated configuration file through the DHCP Server whenever the device reboots. The DHCP server maintains the TFTP Server IP address, where the files are saved. The possible field values are: • *Enabled* — Enables automatic updates from the DHCP server. • *Disabled* — Disables automatic updates from the DHCP server. This is the default value.

2. Select Enabled to turn on DHCP Auto configuration or Disabled to turn it off. Disabled is the default.
3. Click Apply. The DHCP automatic configuration update is modified, and the device is updated.

Dual Image Services

The device contains two software images in its flash memory, one is for reboot and the other one is for backup. When a software download is successfully completed, the new image automatically becomes the new reboot file, unless the user manually configures the other file to be active. In a stacked system, the user can define the active image file for every unit in the stack.

When the user is downloading a new image, it will always be downloaded to the location of the second image. It means that if image1 is the currently running image, the new firmware will be always downloaded as image2, nothing else will happened untill the next reboot.

By default, the newly downloaded image will be marked as the next image which will run after the reboot. However, the user can identify the next image which will run after reboot by viewing the page: 'Dual Image Services/Firmware Information' and change the next image that will run after reboot if user config the page: 'Dual Image Services/Config Firmware Image'.

This feature includes two screens:

- Firmware InformationConfig Firmware Image

Firmware Information

The device contains two software images in its flash memory, one is for bootup and the other one is for backup. When a software download is successfully completed, the new image automatically becomes the active image after the reboot. The user can also manually configure the other file to be the bootup image instead. In a stacked system, the user can define the bootup image file for every unit in the stack.

When the user is downloading a new image, it will always be downloaded to the location of the non-active image. It means that if image1 is the currently active image, the new firmware will be always downloaded as image2.

The user can also delete an image, however only the non-active image can be deleted.

The *Firmware Information Page* contains information about the image files stored for the device, or in case of a stacked system, for all devices in the stack. To view the list of device images:

- Click **Configuration > Dual Image Services > Firmware Information**. The *Firmware Information Page* opens:

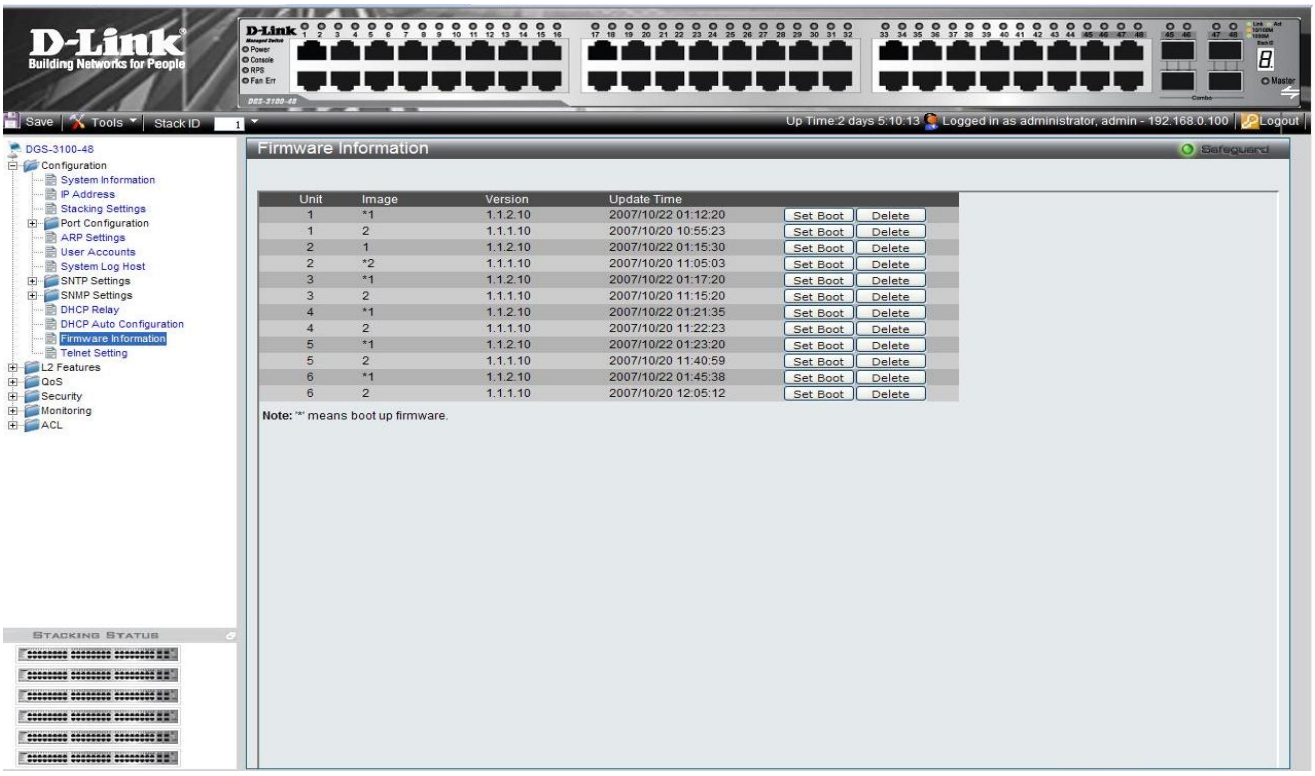


Figure 0-23 Firmware Information Page

The Firmware Information Page contains the following fields:

Field	Description
Unit	Displays the stacking member for which the firmware image information is displayed.
Image	Each device has two image files, one for reboot and one for backup. Upon software upgrade download, the downloaded image file is designated for reboot, although users can modify this in the Config Firmware Image page. An "*" indicates that this image file is used for reboot.
Version	Displays the image file's version number.
Update Time	Displays the time and date which the software was saved to the server.
Set Boot	Selects the image to be become the active image at the next bootup.
Delete	Deletes the selected image. The image is deleted immediately.

Config Firmware Image

The Config Firmware Image Page allows users to change each device's image file. To change the reboot file:

1. Click **Configuration > Dual Image Services > Config Firmware Image**. The *Config Firmware Image Page* opens**:**

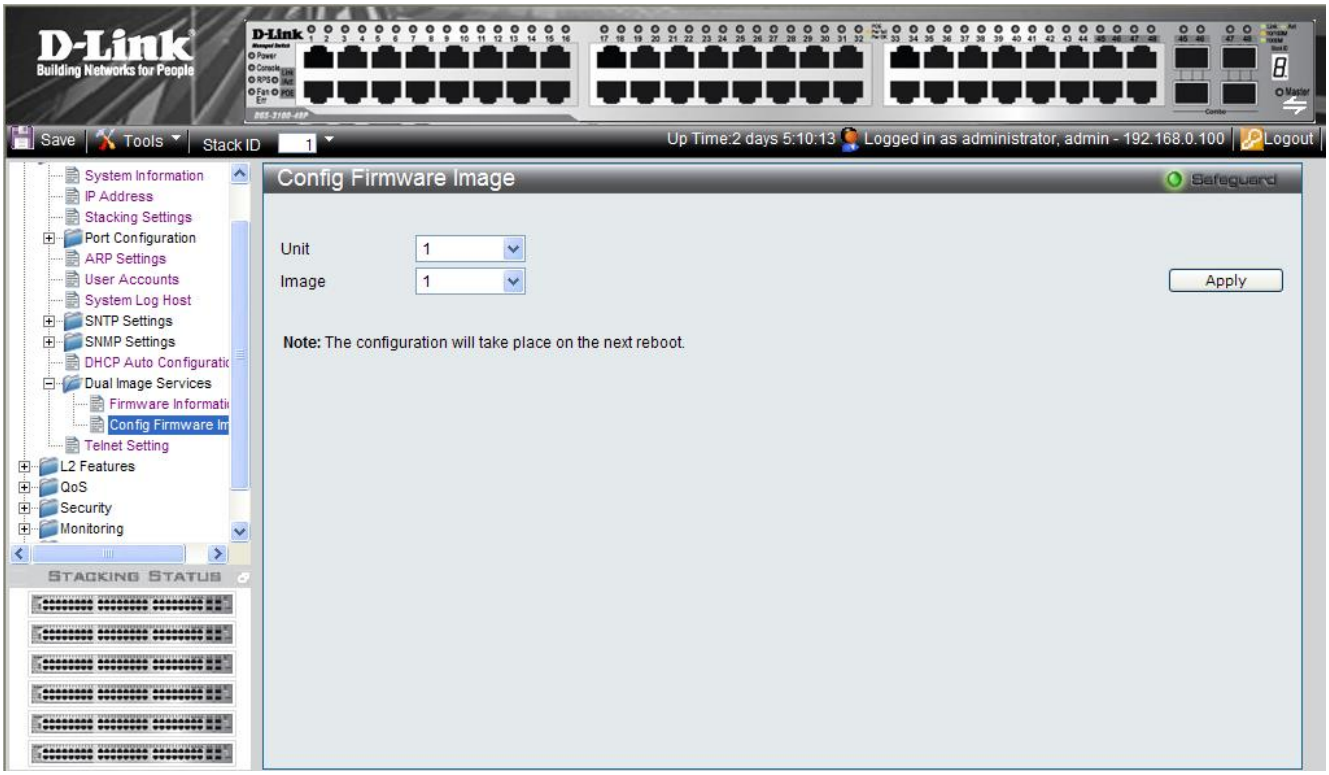


Figure 0-24 Config Firmware Image Page

The Config Firmware Image Page contains the following fields:

Field	Description
Unit	Defines the stacking member for which the reboot image file is defined.
Image	Defines the image file used for reboot. The possible values are: • *1* – Image-1 is the latest downloaded image file. • *2* – Image-2 is the previously downloaded image file.

2. Select the Unit and choose its reboot Image file.
3. Click Apply. The device will use the defined image file to reboot next time.

Telnet Setting

The *Telnet Setting* allows users to enable or disable Telnet on the device. To enable or disable Telnet:

1. Click **Configuration > Telnet Setting**. The *Telnet Setting* opens**:**

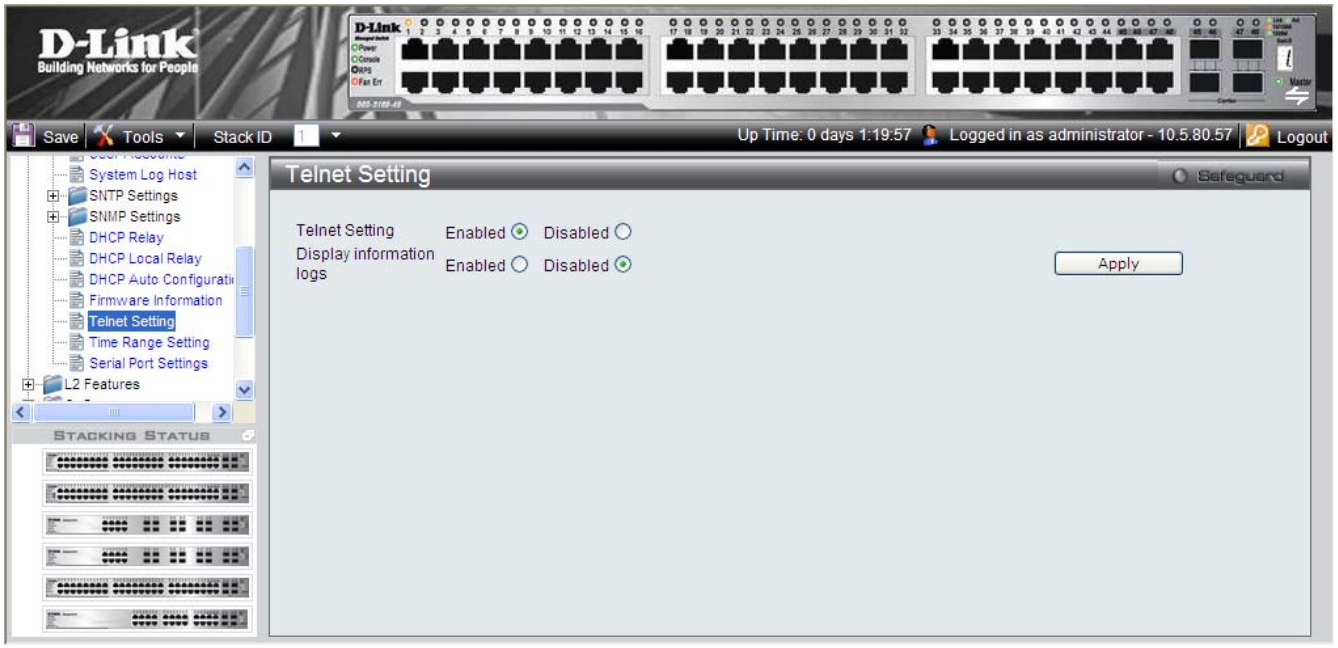


Figure 0-25 Telnet Setting Page

The Telnet Setting contains the following fields:

Field	Description
Telnet Setting	Defines the Telnet status on the device. The possible values are: • *Enabled* – Enables Telnet. • *Disabled* – Disables Telnet.
Display Information Logs	Defines the Telnet logging on the device. The possible values are: • Enabled – Enables all Telnet logging messages to be displayed. • Disabled – Disables Telnet logging so that only high severity messages are displayed. If this is selected, logging on SSH and console sessions is also disabled.

2. Select the Telnet Setting.
3. Click Apply. The Telnet setting on the device is updated.

Defining Time Ranges

Time ranges may be used to define time-based ACLs and to configure time ranges for PoE port settings. The *Time Range Setting Page* defines a time range. To define a time range:

1. Click **Configuration > Time Range Setting**. The *Time Range Setting Page* opens:

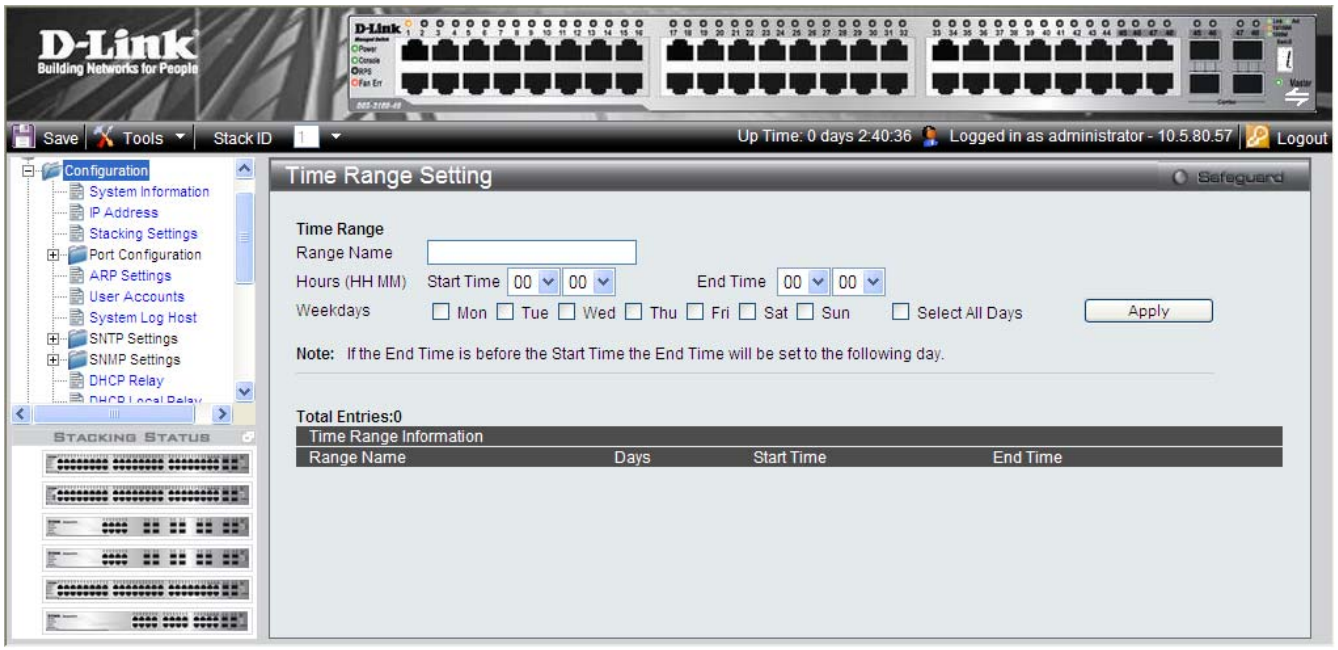


Figure 2-166 Time Range Setting Page

The Time Range Setting Page contains the following fields:

Field	Description
Range Name	Defines the Time Range Name. Up to 32 time ranges can be defined.
Start Time (HH:MM)	Specifies the time at which the time-based feature is enabled. The field format is HH:MM. The possible field values are: • HH: 00 – 23 (hours, in military format) • MM: 00 – 59 (minutes)
End Time (HH:MM)	Specifies the time at which the time-based feature is disabled. The field format is HH:MM. The possible field values are: • HH: 00 – 23 (hours, in military format) • MM: 00 – 59 (minutes)
Weekdays	Specifies the weekdays for which the time range applies.
Select All Days	Specifies that the time range is applied daily.

2. Define the Range Name, Start Time and End Time fields.
3. To define the applicable days, check the specific *Weekdays* or check *Select All Days*.
4. Click Apply. The Time Range is defined.

To delete a Time Range entry:

1. Select the entry.
2. Click Delete. A confirmation window is displayed .
3. Click OK. The entry is deleted.

To view or modify Time Range settings:

1. Click Edit. The **Time Range Edit Page** *Time Range Edit Page* opens:

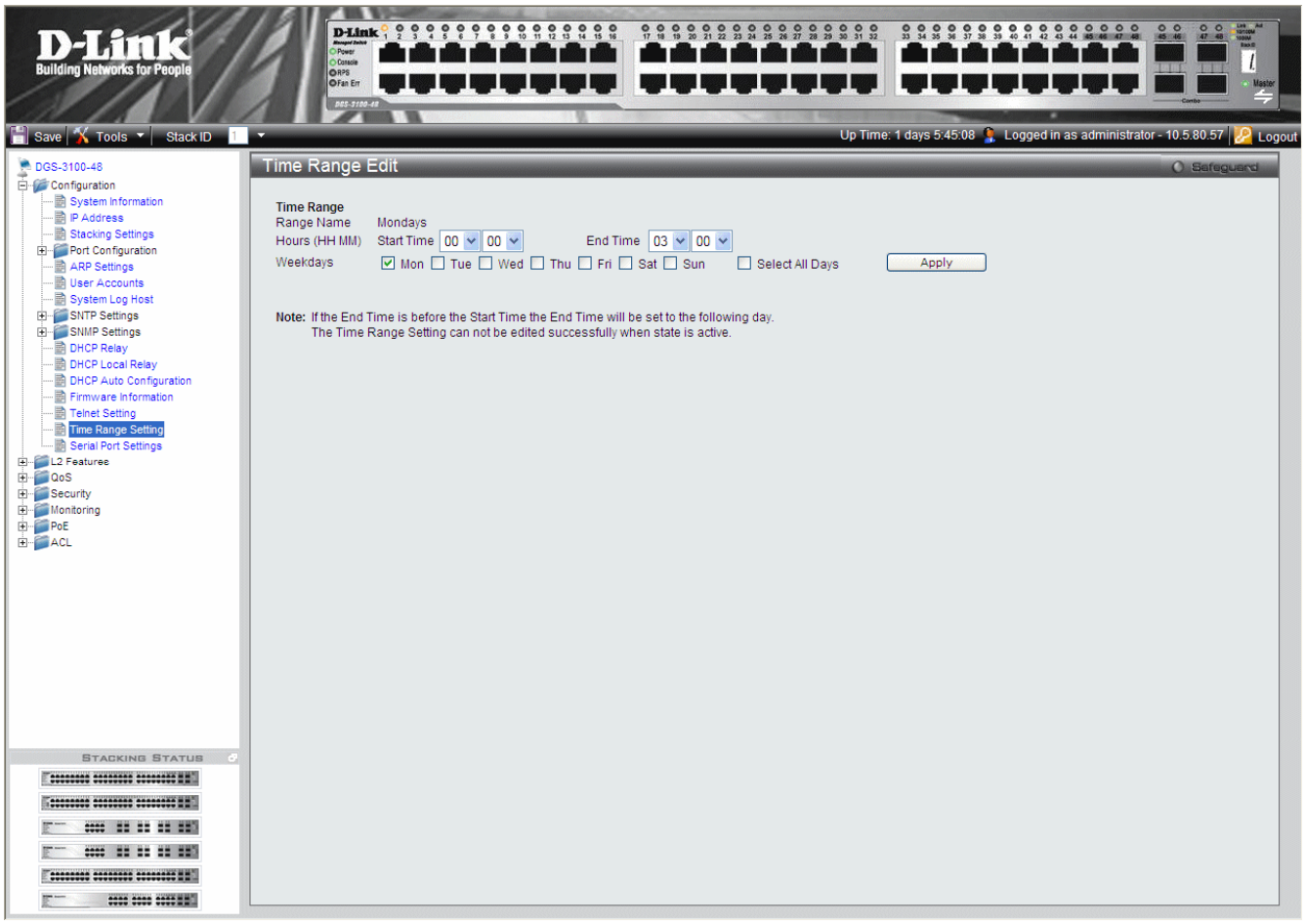


Figure 2-177 Time Range Edit Page

2. Define the *Time Range Edit* fields.
3. Click Apply. The time range is modified, and the device is updated

Serial Port Settings

The *Serial Port Settings* enables users to configure access to the device via a serial port.

To configure serial port access:

1. Click **Configuration > Serial Port Settings**. The *Serial Port Settings Page* opens:

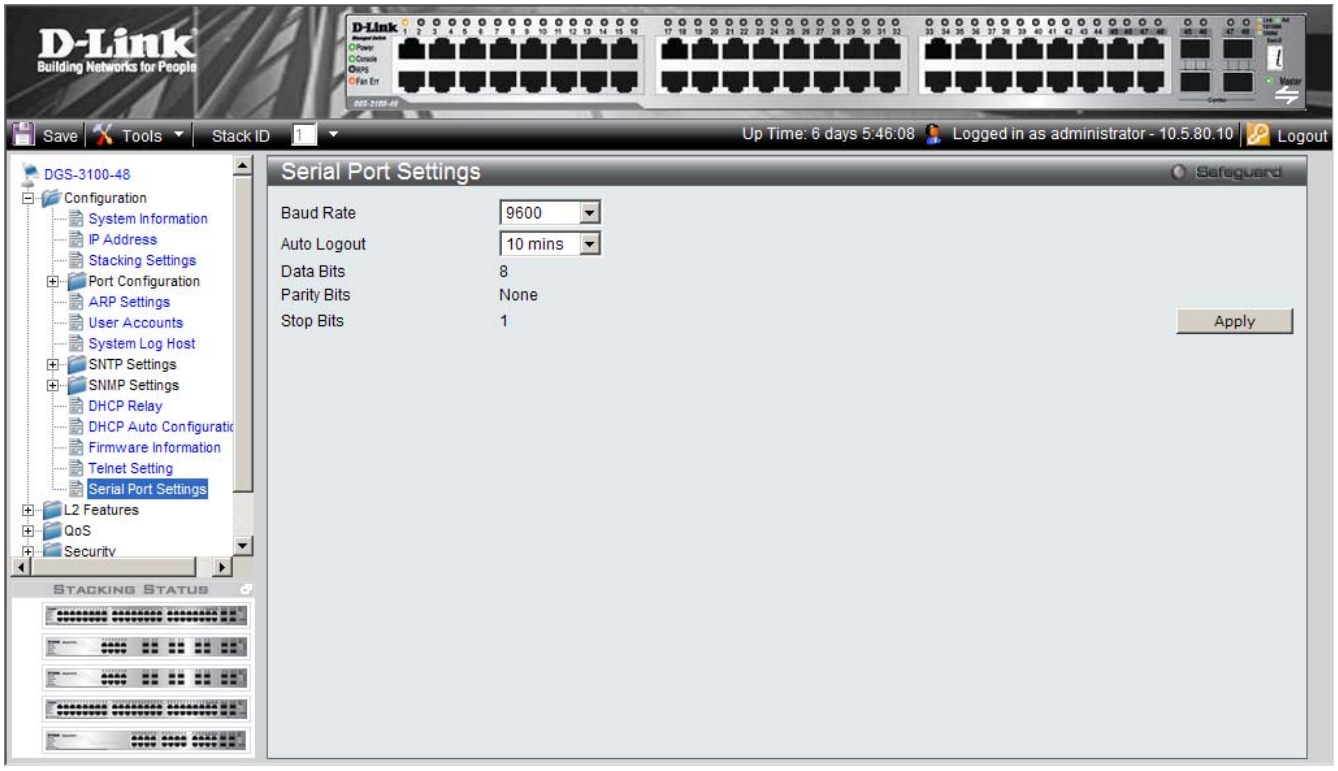


Figure 0-188 Serial Port Settings Page

The Serial Port Page contains the following fields:

Field	Description
Baud Rate	Defines the Baud Rate on the device. The possible values are: • 2400 • 4800 • 9600 • 19200 • 38400
Auto Logout	Defines the allowable inactivity length before the device automatically logs out. The possible values are: • Never • 2 min • 5 min • 10 min • 15 min

2. Select the appropriate values.
3. Click Apply. The Serial Port Settings on the device are updated.

3

CONFIGURING L2 FEATURES

This section contains information for enabling and configuring L2 Features. This section contains the following topics:

- Enabling Jumbo Frames
- Configuring VLANs
- Configuring GVRP
- Defining Trunking
- Traffic Segmentation
- Configuring LACP
- Defining IGMP Snooping
- Defining MLD Snooping
- Configuring Port Mirroring
- Configuring Spanning Tree
- Defining Forwarding and Filtering
- Configuring LLDP
- Configuring Voice VLAN
-

Enabling Jumbo Frames

Jumbo Frame support is designed to enhance Ethernet networking throughput and significantly reduce the CPU utilization of large file transfers like large multimedia files or large data files by enabling more efficient larger payloads per packet. The *Jumbo Frame Page* allows network managers to enable Jumbo Frames on the device.

1. Click **L2 Features > Jumbo Frame.** The *Jumbo Frame Page* opens**:**

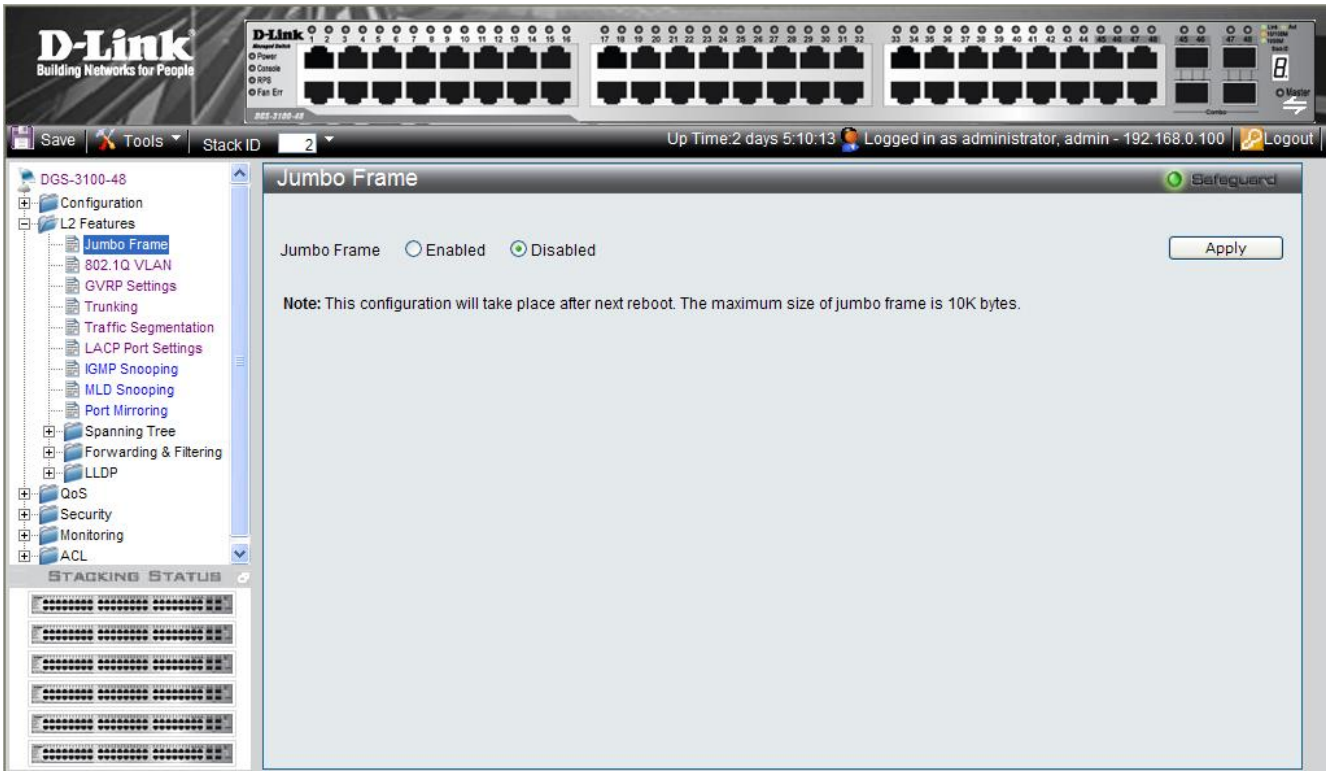


Figure 0–1 Jumbo Frame Page

The Jumbo Frame Page contains the following field:

Field	Description
Jumbo Frame	Defines whether Jumbo Frames are enabled on the device. The possible field values are: *Enabled* — Enables Jumbo Frames on the device. *Disabled* — Disables Jumbo Frames on the device. This is the default value.

2. Select *Enable* in the *Jumbo Frames* field. Jumbo Frames are enabled only after the configuration is saved and the device is rebooted.
3. Click Apply. Jumbo Frames are enabled after the device is reset.

Configuring VLANs

Understanding IEEE 802.1p Priority

Priority tagging is an IEEE 802.1p defined standard function designed to provide a means of managing traffic on networks where many different types of data are transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time-critical data over congested networks. The quality of applications dependent on such data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

IEEE 802.1p standard-compliant network devices recognize the priority level of data packets and can assign priority labels or tags to packets, as well as strip priority tags from packets. The priority tag determines the packet's degree of expeditiousness and the queue to which it is assigned.

Priority tags are assigned values from 0 to 7, with 0 being assigned to the lowest priority data, and 7 to the highest. Generally, tag 7 is used for data associated with video or audio applications, sensitive to even slight delays, or for data from specified end users whose data transmissions warrant special consideration.

The switch enables increased definition for handling priority tagged data packets on the network. Using queues to manage priority tagged data enables user-specification for the data's relative priority to suit the needs of the network. Circumstances can arise where it is advantageous to group two or more differently tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 3, be reserved for data packets with a priority value of 7.

A weighted round robin system is employed on the switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 8:1. This means that the highest priority queue, Queue 3, clears eight packets for every one packet cleared from Queue 0.

It is important that the priority queue settings on the switch are for all ports, and all devices connected to the switch are affected. The priority queuing system is especially beneficial for networks that employ priority tag assignment capable switches.

VLAN Description

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLANs also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Notes about VLANs on the DGS-3100 Series

No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.

The DGS-3100 series supports IEEE 802.1Q VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.

The switch's default is to assign all ports to a single 802.1Q VLAN named 'default.'

The 'default' VLAN has a VID = 1.

IEEE 802.1Q VLANs

Some relevant terms:

Term	Description
Tagging	The act of putting 802.1Q VLAN information into the header of a packet.

Term	Description
Untagging	The act of stripping 802.1Q VLAN information out of the packet header.
Ingress port	A port on a switch where packets are flowing into the switch and VLAN decisions must be made.
Egress port	A port on a switch where packets are flowing out of the switch, either to another switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the switch. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN are only forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLANs can also provide a level of security to a network. IEEE 802.1Q VLANs only deliver packets between stations that are members of the VLAN.

Any port can be configured as either tagged or untagged. The untagging feature of IEEE 802.1Q VLANs allows VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

The IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN in which the receiving port is a member.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns packets to VLANs by filtering.
- Assumes the presence of a single global spanning tree.
- Uses an explicit tagging scheme with one-level tagging.
- 802.1Q VLAN Packet Forwarding

Packet forwarding decisions are made based upon the following three types of rules:

- Ingress rules - rules relevant to the classification of received packets belonging to a VLAN.
- Forwarding rules between ports - decides whether to filter or forward the packet.
- Egress rules - determines if the packet must be sent tagged or untagged.

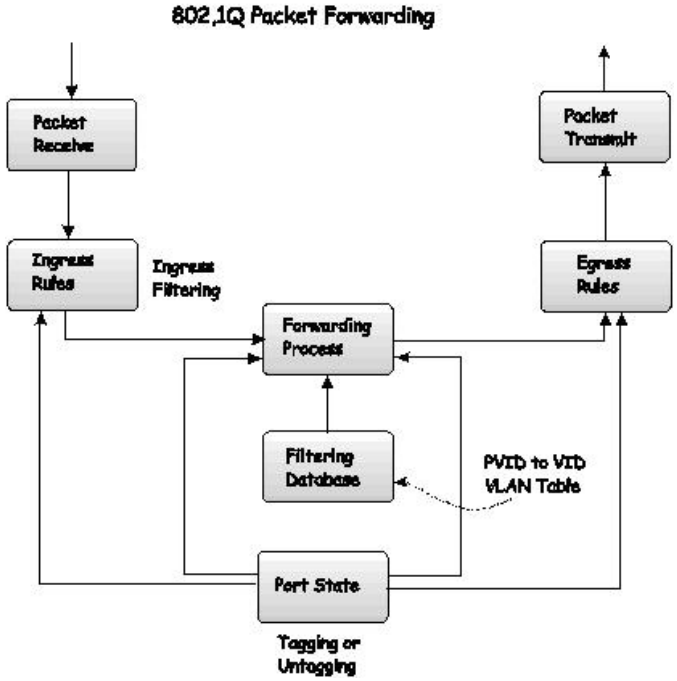


Figure 0–2 IEEE 802.1Q Packet Forwarding

802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's EtherType field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating token ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

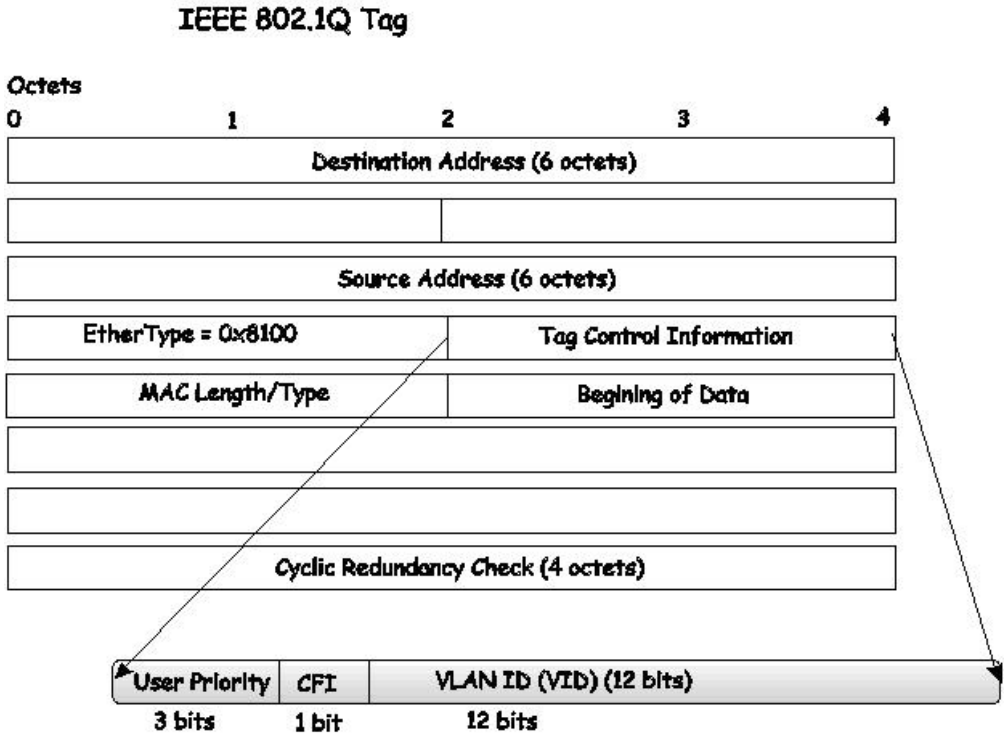


Figure 0–3 IEEE 802.1Q Tag

The EtherType and VLAN ID are inserted after the MAC source address, but before the original EtherType/Length or Logical Link Control. Due to the packet now being a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

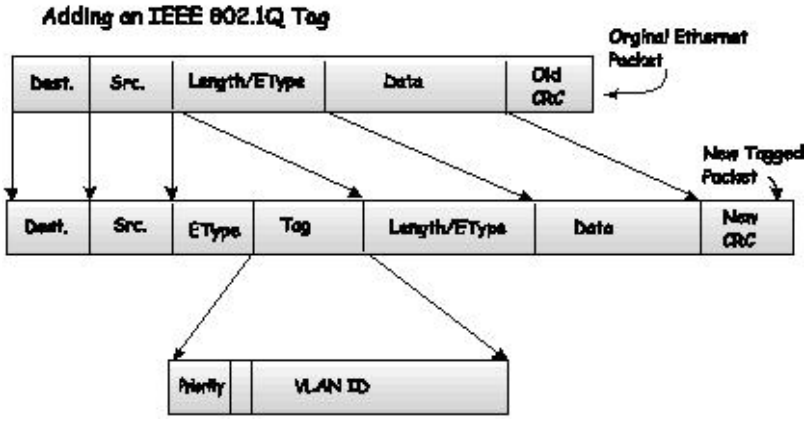


Figure 0–4 Adding an IEEE 802.1Q Tag

Port VLAN ID

Tagged packets (carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and the entire network, providing all network devices are 802.1Q compliant).

Not all network devices are 802.1Q compliant. Such devices are referred to as tag-unaware. 802.1Q devices are referred to as tag-aware.

Prior to the adoption of 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponds to the packet's destination address (found in the switch's forwarding table). If the PVID of the port receiving the packet is different from the PVID of the port that is to transmit the packet, the switch drops the packet.

Within the switch, different PVIDs mean different VLANs (remember that two VLANs cannot communicate without an external router). So, VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given switch (or switch stack).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLANs are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVIDs within the switch to VIDs on the network. The switch compares the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the switch drops the packet. As a result of the existence of the PVID for untagged packets, and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can only have one PVID, but it can have as many VIDs that the switch’s memory storage capacity has in its VLAN table, to store them.

As some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted; Should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Tagging and Untagging

Every port on an 802.1Q compliant switch can be configured as tagged or untagged.

Tagging enabled ports put the VID number, priority, and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port does not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag is then used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.

Ports with untagging enabled strip the 802.1Q tag from all packets flowing into and out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port does not alter the packet. As a result, all packets received by and forwarded by an untagging port have no 802.1Q VLAN information (as the PVID is only used internally within the switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Ingress Filtering

A port on a switch where packets are flowing into the switch, and VLAN decisions must be made, is referred to as an ingress port. If ingress filtering is enabled for a port, the switch examines the VLAN information in the packet header (if present) and decides whether or not to forward the packet.

If the packet is tagged with VLAN information, the ingress port first determines if the ingress port itself is a member of the tagged VLAN. If it is not, the packet is dropped. If the ingress port is a member of the 802.1Q VLAN, the switch determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port tags the packet with its own PVID as a VID (if the port is a tagging port). The switch then determines if the destination port is a member of the same VLAN (has the same VID) as

the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded and the destination port transmits it on its attached network segment.

This process is referred to as ingress filtering, and is used to conserve bandwidth within the switch, by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that is just dropped by the destination port.

Default VLANs

The switch initially configures one VLAN, VID = 1, called 'default.' The factory default setting assigns all ports on the switch to the 'default.'

Ports can be removed from the default VLAN by either setting the port on the default VLAN as a non-member, or if the port is configured as Untagged on another VLAN.

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

NOTE: If no VLANs are configured on the switch, then all packets are forwarded to any destination port. Packets with unknown source addresses are flooded to all ports. Broadcast and multicast packets are also flooded to all ports.

An example is presented in this table:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4

Table 0-1 VLAN Example - Assigned Ports

VLAN and Trunk Groups

Trunk Groups (LAGs) can be added as member to a VLAN (similar to ports).

The members of a trunk group have the same VLAN setting. Any VLAN setting on trunk group members applies to the other member ports.

NOTE: In order to use VLAN segmentation in conjunction with port trunk groups, the port trunk group(s) can first be set, and then the VLAN settings may be configured. Changing the port trunk grouping with VLANs already in place doesn't require reconfiguration of the VLAN settings after changing the port trunk group settings. VLAN settings automatically change in conjunction with the change of the port trunk group settings.

VLAN Status

The VLAN List displays VLANs, VLAN membership and membershiop type. This window displays the ports on the switch that are currently Egress or Tag ports. To view the following table, open the L2 features->VLAN folder and click the VLAN Status Link.

This section contains the following topics:

- Defining VLAN Properties
- Configuring GVRP

Defining VLAN Properties

The *VLAN Configuration Page* provides information and global parameters for configuring and working with VLANs.

1. Click **L2 Features > 802.1Q VLAN**. The *VLAN Configuration Page* opens**:**

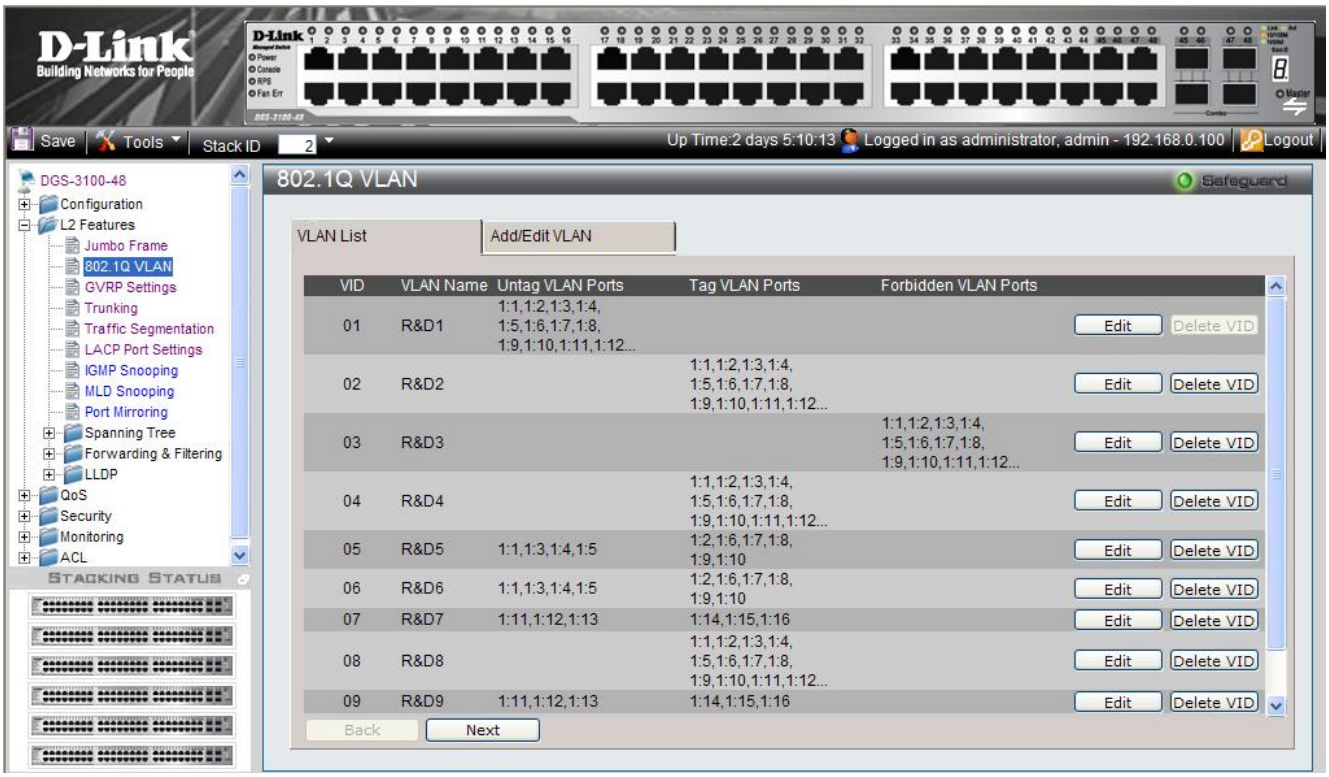


Figure 0–5 VLAN Configuration Page

The VLAN Configuration Page contains the following fields:

Field	Description
VID	Defines the VLAN ID.
VLAN Name	Defines the user-defined VLAN name. The field ranges is 1-32 characters.
Untag VLAN Ports	Defines the interface is an untagged VLAN member. Packets forwarded by the interface are untagged.
Tag VLAN Ports	Defines the interface is a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
Forbidden VLAN Ports	Defines the interface VLAN membership, even if GVRP indicates the port is to be added.

NOTE: The Guest VLAN should be disabled before deleting the VLAN which was defined as the Guest VLAN.

NOTE: On the Default VLAN, the user can define ports as ‘Untagged’ or ‘Tagged’ but not as ‘Forbidden’.

2. Click the Add/Edit VLAN tab. The *Add/Edit VLAN Information Page* opens:

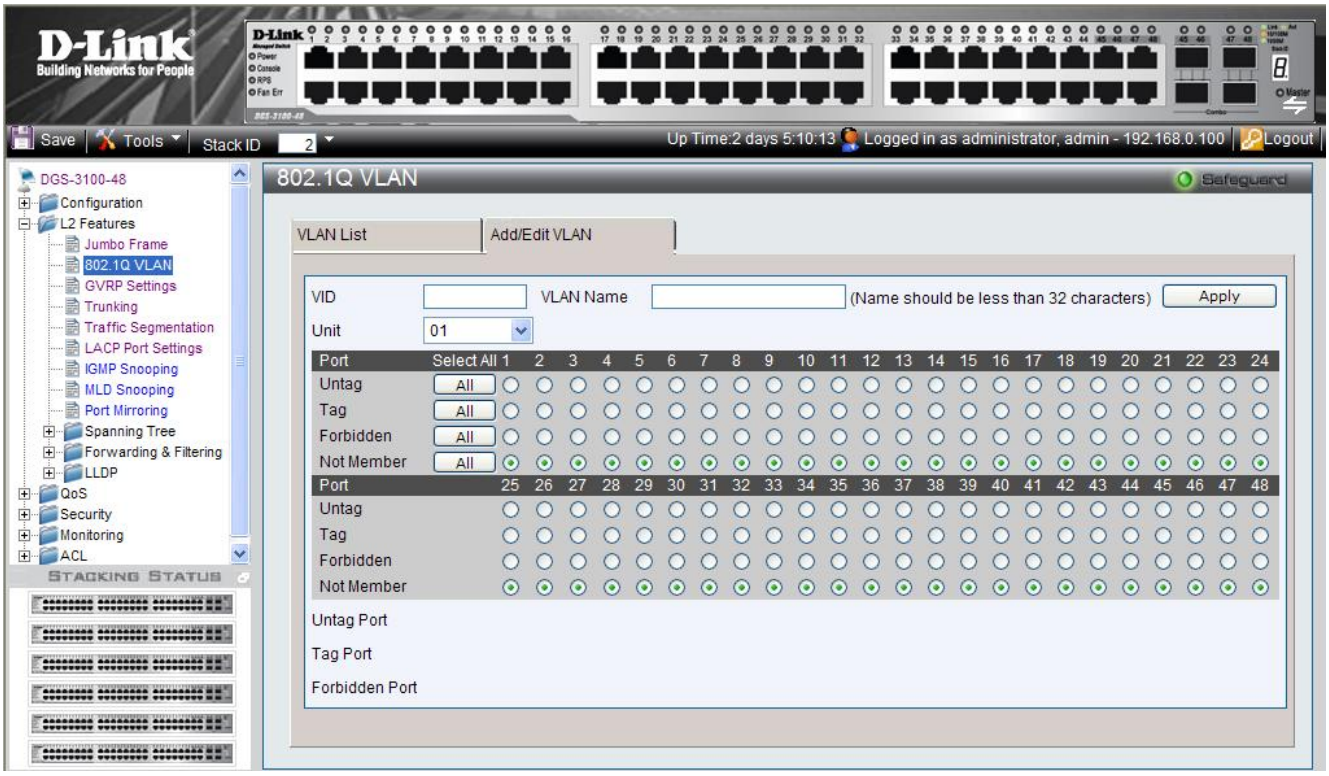


Figure 0–6 Add/Edit VLAN Information Page

The Add/Edit VLAN Information Page contains the following fields:

Field	Description
VID	Defines the VLAN ID.
VLAN Name	Defines the user-defined VLAN name. The field ranges up to 32 characters.
Unit	Defines the stacking member for which the VLAN parameters are displayed.
Untag Port	Defines the interface is an untagged VLAN member. Packets forwarded by the interface are untagged.
Tag Port	Defines the interface is a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
Forbidden Port	Defines the interface VLAN membership, even if GVRP indicates the port is to be added.
Not Member	Indicates that the interface is not a member of the VLAN.
Port Select All	Selects all ports and either untags, tags, excludes, or removes the VLAN membership.

3. Define the *VID*, *VLAN Name*, and *port-related* fields.
4. Select the *Tagged*, *Untagged*, and *Forbidden* ports.
5. Click Apply. The VLAN is saved, and the device is updated.

To modify a VLAN:

1. Click L2 Features > 802.1Q VLAN. The VLAN Configuration Page opens:
2. Select a VLAN in the VLAN Table.
3. Click Edit. The configured VLAN parameters are displayed in the *Add/Edit VLAN Information* section.
4. Modify the VLAN parameters.
5. Click Apply. The VLAN information is modified, and the device is updated.

Defining Asymmetric VLAN

The device configuration allows a port to be defined as an untagged member only in one VLAN and tagged in multiple VLANs. By enabling Asymmetric VLAN on the device, a port is defined as an untagged member in multiple VLANs. This allows ports from separate VLANs access to a remote server without accessing other hosts.

When Assymetric VLAN is enabled, if a port is an untagged member in VLAN #1, VLAN #1 must be the PVID.

The following scenerio illustrates the feature:

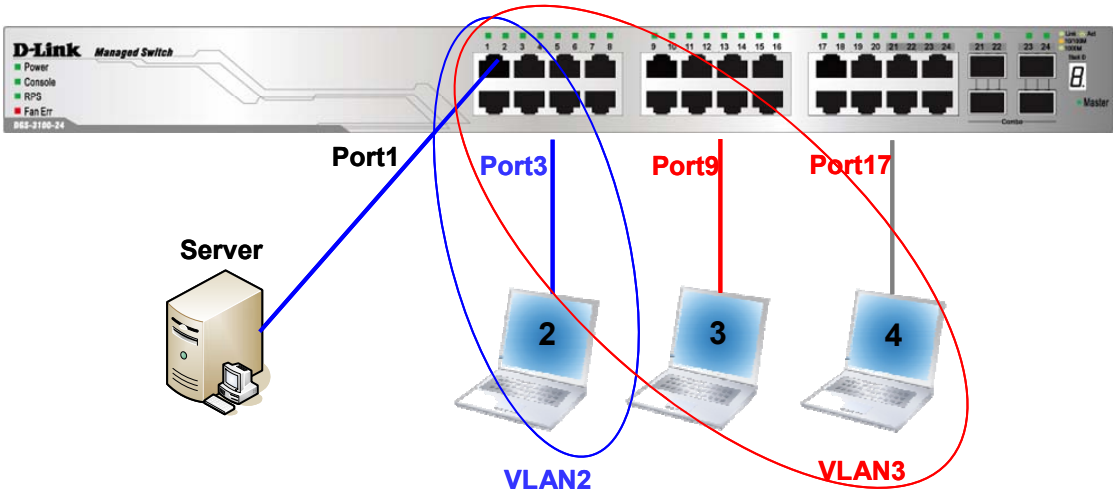


Figure 0–7 Asymmetric VLAN scenerio

Port 1 connect to Server; port 1, port 3, port 9 and port 17 are untagged ports; PC3 & PC4 are in the same VLAN#3; port 1 is a untagged member of VLAN#2 and VLAN#3 (untagged member overlap). Then the server can talk with VLAN#2, VLAN#3; PC3 and PC4 can talk to the server and to each other; PC2 can talk to the Server; VLAN#2 can't communicate with VLAN3.

In this example port 1 need to be untagged member in VLAN#2 & VLAN#3, so Asymmetric VLAN should be enabled

NOTE: In order to support this network scenario, the user will need to activate also 'DLF Filtering' feature which will be released in DGS-3100-xx R3.0 as well

The default VLAN (VID=1) cannot be used as shared VLAN.

1. Click **L2 Features >Asymmetric VLAN**. The *Asymmetric VLAN* **Page** opens**:**

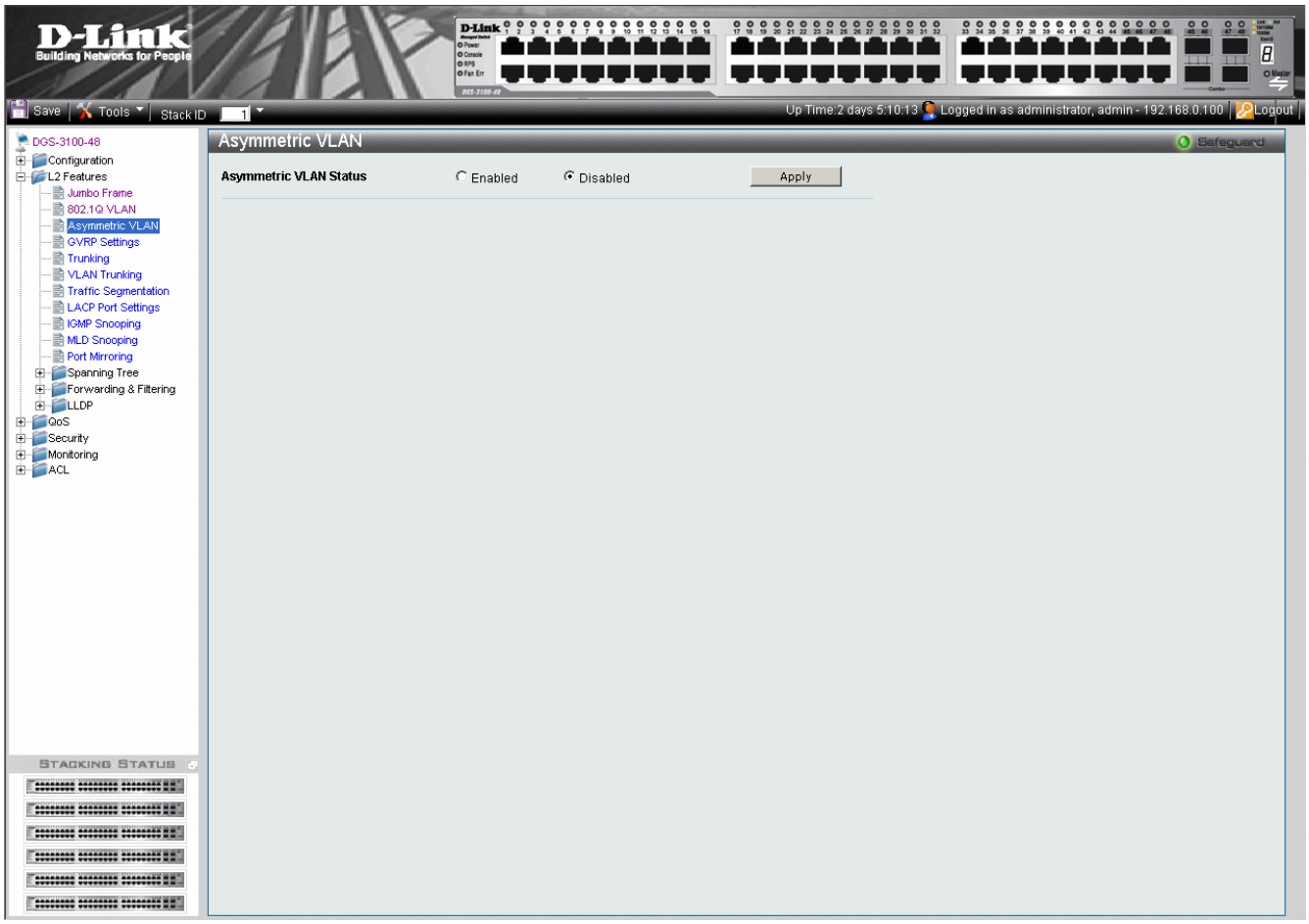


Figure 0–8 Asymmetric VLAN Page

The Asymmetric VLAN Page contains the following fields:

Field	Description
Asymmetric VLAN Status	Defines whether Asymmetric VLAN is enabled on the device. The possible field values are: *Enabled* — Enables Asymmetric VLAN on the device. *Disabled* — Disables Asymmetric VLAN on the device. This is the default value.

2. Select Enabled/Disabled in the *Asymmetric VLAN Status* field.
3. Select Enable in the DLF Filtering (see Defining DLF Filtering).
4. Click Apply. The Asymmetric VLAN option is enabled, and the device is updated.

Configuring GVRP

GVRP timers need to be in the default values on all Layer 2-connected devices. If the GVRP timers are set differently on the Layer 2-connected devices, the GVRP application does not operate successfully.

GARP VLAN Registration Protocol (GVRP) is specifically provided for automatic distribution of VLAN membership information between VLAN-aware bridges. GVRP allows VLAN-aware bridges to automatically learn VLANs to bridge port mapping without requiring the individual configuration of each bridge and register VLAN membership. To define GVRP on the device:

1. Click **L2 Features > GVRP Settings**. The *GVRP Setting Page* opens**:**

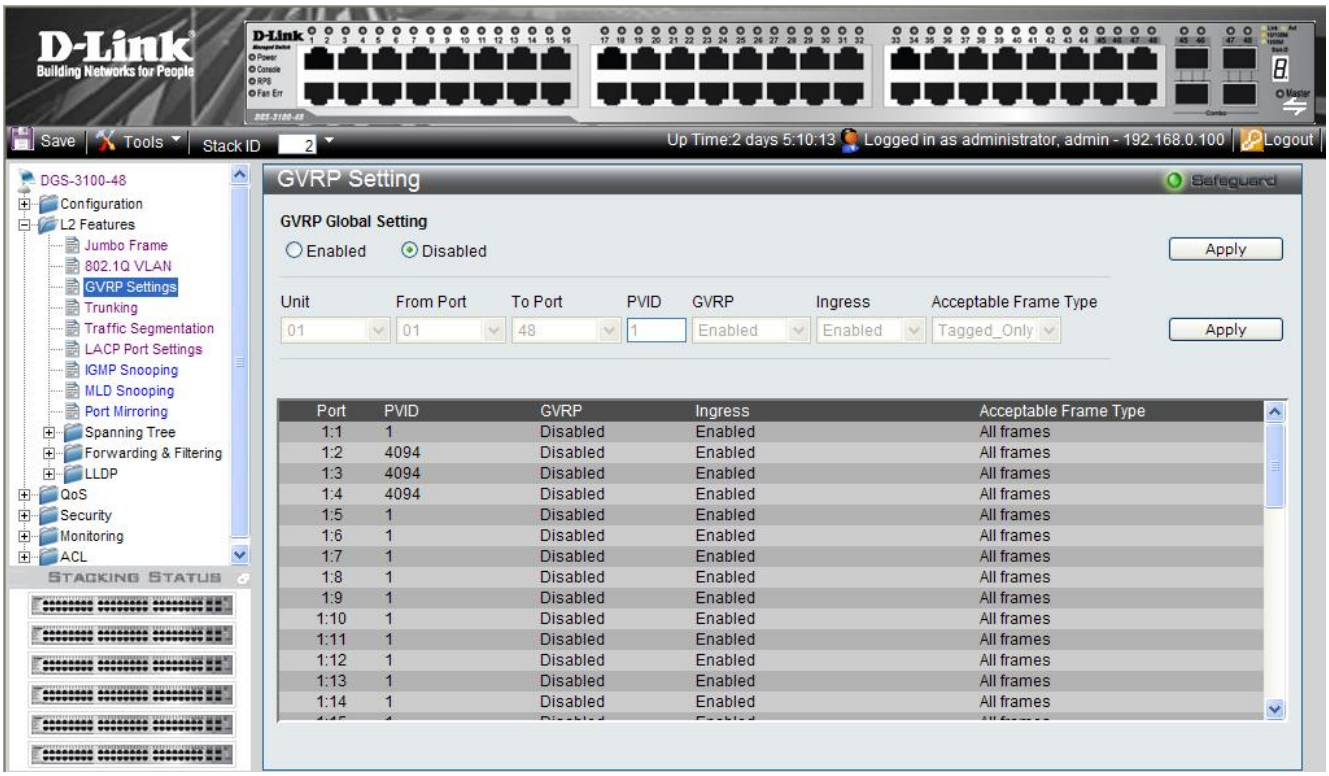


Figure 0–9 GVRP Setting Page

The GVRP Setting Page contains the following fields:

Field	Description
GRVP Global Setting	Defines whether GRVP is enabled on the device. The possible field values are: *Enabled* — Enables GRVP on the device. *Disabled* — Disables GRVP on the device. This is the default value.
Unit	Defines the stacking member's Unit ID and LAGs for which GVRP parameters are displayed.
From Port	Defines the first port number that is displayed to which GVRP are assigned.
To Port	Defines the last port number that is displayed to which GVRP are assigned.
PVID	Defines the PVID assigned to the port.
GVRP	Defines whether GVRP is enabled on the port. The possible field values are: *Enabled* — Enables GVRP on the selected port. *Disabled* — Disables GVRP on the selected port. (This is the default value).
Ingress	Defines whether Ingress filtering is enabled on the device. The possible field values are: *Enabled* — Enables Ingress filtering on the device. Ingress filtering compares an incoming VID tag packet with the PVID number assigned to the port. If the PVIDs vary, the port drops the packet. (This is the default value). *Disabled* — Disables Ingress filtering on the device.
Acceptable Frame Type	Defines the packet type accepted on the port. The possible field values are: *Admit Tagged Only* —Only tagged packets are accepted on the port. *Admit All* — Both tagged and untagged packets are accepted on the port. (This is the default value).

2. Select a stacking member in the *Unit* field.
3. Select the ports to and from which the GVRP parameters are displayed in the *From/To Port* fields.
4. Define the PVID, GVRP, Ingress, and Acceptable Frame Type fields.
5. Click Apply. The GVRP is enabled, and the device is updated.

NOTE: When GVRP is globally enabled, GVRP is enabled on all the ports. Users can still disable the GVRP state on a per-port basis.

Defining Trunking

The *Trunking Configuration Page* contains information for assigning ports to LAGs and defining LAG parameters.

Load Balancing

Traffic forwarded to the trunk interface (LAG) is load-balanced across the physical links, thus achieving an effective bandwidth close to the aggregate bandwidth of each of the port members of the trunk group (LAG).

Traffic load balancing over trunk groups is managed by a hash-based distribution function that distributes Unicast traffic based on Layer 2 or Layer 3 packet header information. Multicast traffic always uses a single, unique LAG member.

The information used for the trunk is as follows:

- Layer 2 — MAC source and destination addresses
- Layer 3 — IP source and destination addresses

Layer 2 and layer 3 can be used either separately or together, as needed.

A hash function based on the above criteria is calculated and saved in the packet descriptor. The egress process uses this hash function to select the specific trunk group member as the egress destination link. The hash algorithm ensures that the order of packets within a specific flow is preserved

To assign ports to LAGs:

1. Click **L2 Features > Trunking**. The *Trunking Configuration Page* opens**:**

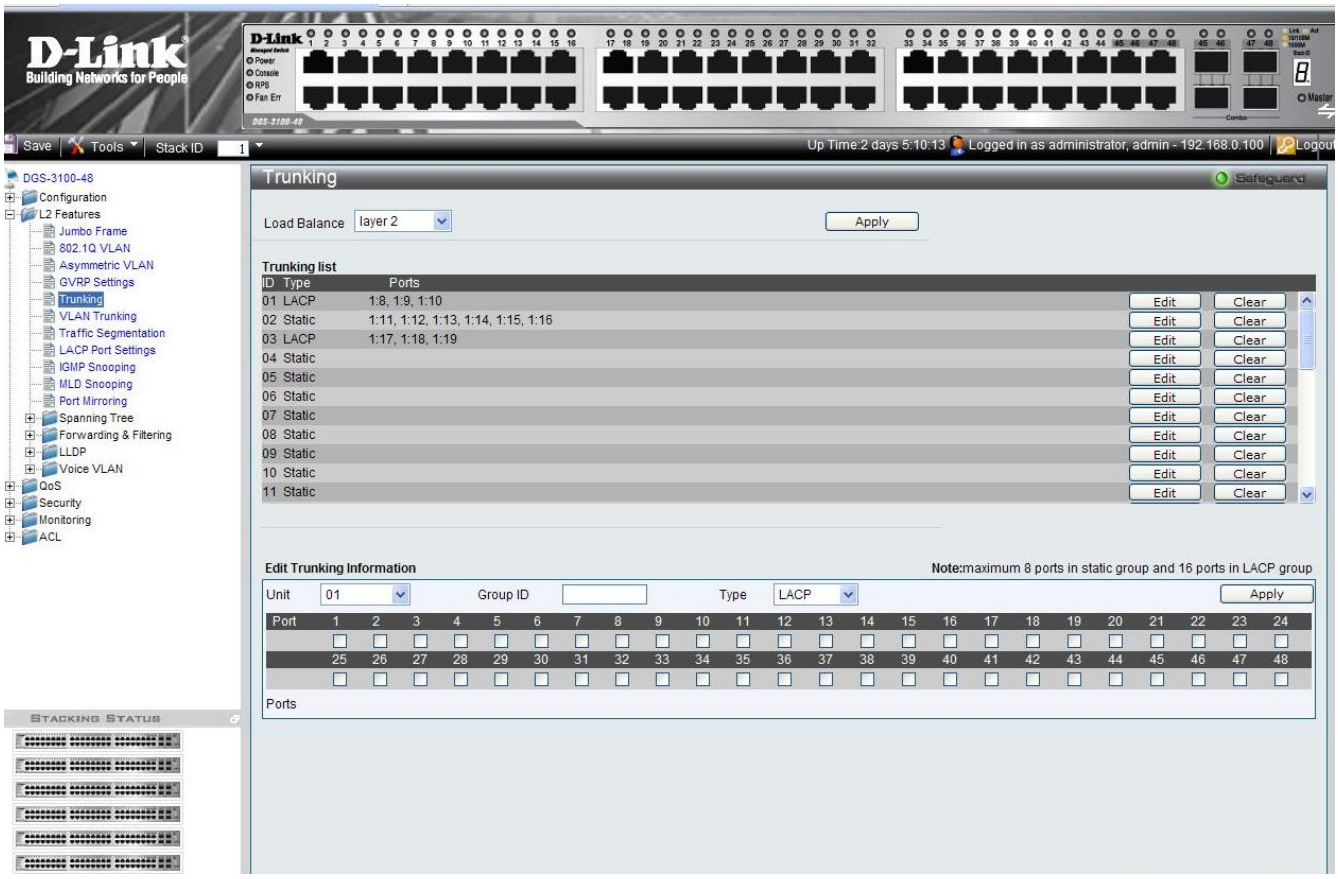


Figure 0–10 Trunking Configuration Page

The Trunking Configuration Page contains the following fields:

Field	Description
Unit	Defines the stacking member's Unit ID for which LAG parameters are displayed.
Load Balance	Defines the method used for load balancing over physical links. This allows for effective port

Field	Description
	bandwidth management. The possible field values are: • Layer 2 — Load balance is achieved using the source and destination MAC addresses. • Layer 3 — Load balance is achieved using the source and destination IP addresses. • Layer 2/3 — Load balance is achieved using the source and destination MAC and IP addresses.
Group ID	Displays the LAG number.
Type	Defines the LAG type. The possible field values are: *Static* — The LAG is static; LACP is disabled on the LAG. (This is the default value). *LACP* — LACP is enabled on the device..
Ports	Displays the ports which are included in the LAG.

2. Select a stacking unit in the *Unit* field.
3. Select the *Load Balance* to use.
4. Define the *Group ID* and *Type* fields.
5. Check the ports to be added to the LAG. The port numbers are displayed in the *Ports* field.
6. Click Apply. The LAG settings are saved, and the device is updated**.**

Notes about Trunking on the DGS-3100 Series

DGS-3100 series supports up to 32 LAGs per device (or stack).

NOTE: A port must belong to the default VLAN when the user is adding the port to a LAG, After adding the port to the LAG, the LAG itself can be joined to other VLAN.

When a port is added to a LAG, the port's configuration is stopping to be active, this configuration will return to be active only after the port will be removed from the LAG.

Defining VLAN Trunking

VLAN Trunking allows frames belonging to unknown VLAN groups to pass through the switch. VLAN Trunking is activated by enabling VLAN Trunking on the device and defining up to 48 ports as “Uplink” ports. In addition, Ingress Filtering must be enabled on all ports (see GVRP Setting Page).

The following limitations are applied to the user-defined Uplink ports:

The Uplink ports can be defined only on Units 1-2 on a stacking device.

The Uplink ports can not be added to a LAG.

The Port Lock option is disabled on both ports.

Port Mirroring is disabled on both ports.

The pass through functionality applies to all VLANs that were not created on the switch, for example if only VLAN #1 is defined on the switch, VLANs 2-4094 will pass traffic between the Uplink ports.

In the example below, the user defined ‘VLAN Trunking’ ports (Uplinks) are ports 23 and 24. In this case, the packet belonging to VLAN 500 enters port 23, defined as one of the Uplink Ports, and therefore will be forwarded to port 24.

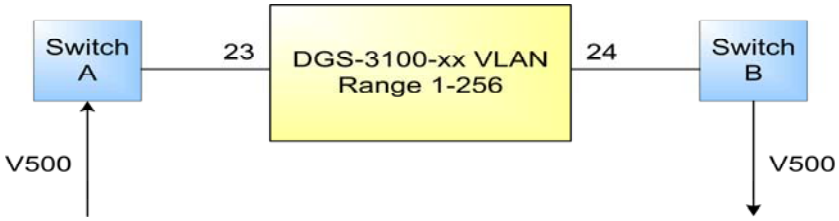


Figure 0–11 VLAN Trunking example between 2 switchs

To define VLAN Trunking on the device:

1. Click **L2 Features > VLAN Trunking**. The *VLAN Trunking Page* opens**:**

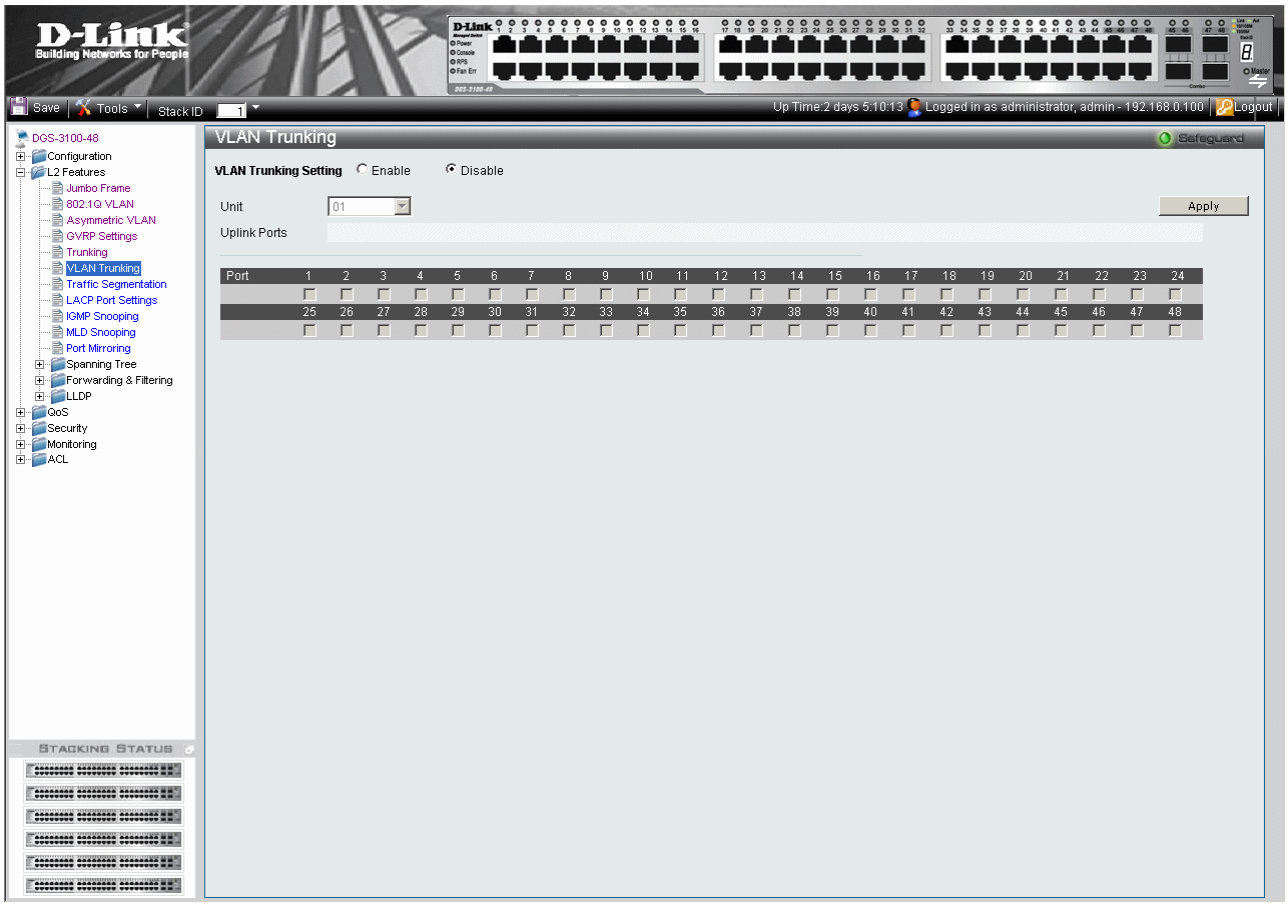


Figure 0–12 VLAN Trunking Page

The VLAN Trunking Page contains the following fields:

Field	Description
VLAN Trunking Setting	Defines whether VLAN Trunking Settings are enabled on the device. The possible field values are: *Enable* — Enables VLAN Trunking Settings on the device. *Disable* — Disables VLAN Trunking Settings on the device. This is the default value.
Unit	Defines the stacking member's Unit ID for which VLAN Trunking parameters are displayed
Uplink Ports	Displays the Uplink ports which are included in the VLAN Trunking.
Ports	Displays the ports which are included in VLAN Trunking.

2. Enable VLAN Trunking.
3. Select a stacking unit in the *Unit* field.
4. Check the ports to be added to the VLAN Trunking. The port numbers are displayed in the *Uplink Ports* field.
5. Click Apply. The VLAN Trunking settings are saved, and the device is updated

Traffic Segmentation

The *Traffic Segmentation Page* enables administrators to force traffic from *source* ports to bypass the Forwarding Database (FDB), and forward all Unicast, Multicast and Broadcast traffic to the *forwarding* port.

To define Traffic Segmentation:

1. Click **L2 Features > Traffic Segmentation**. The *Traffic Segmentation Page* opens:

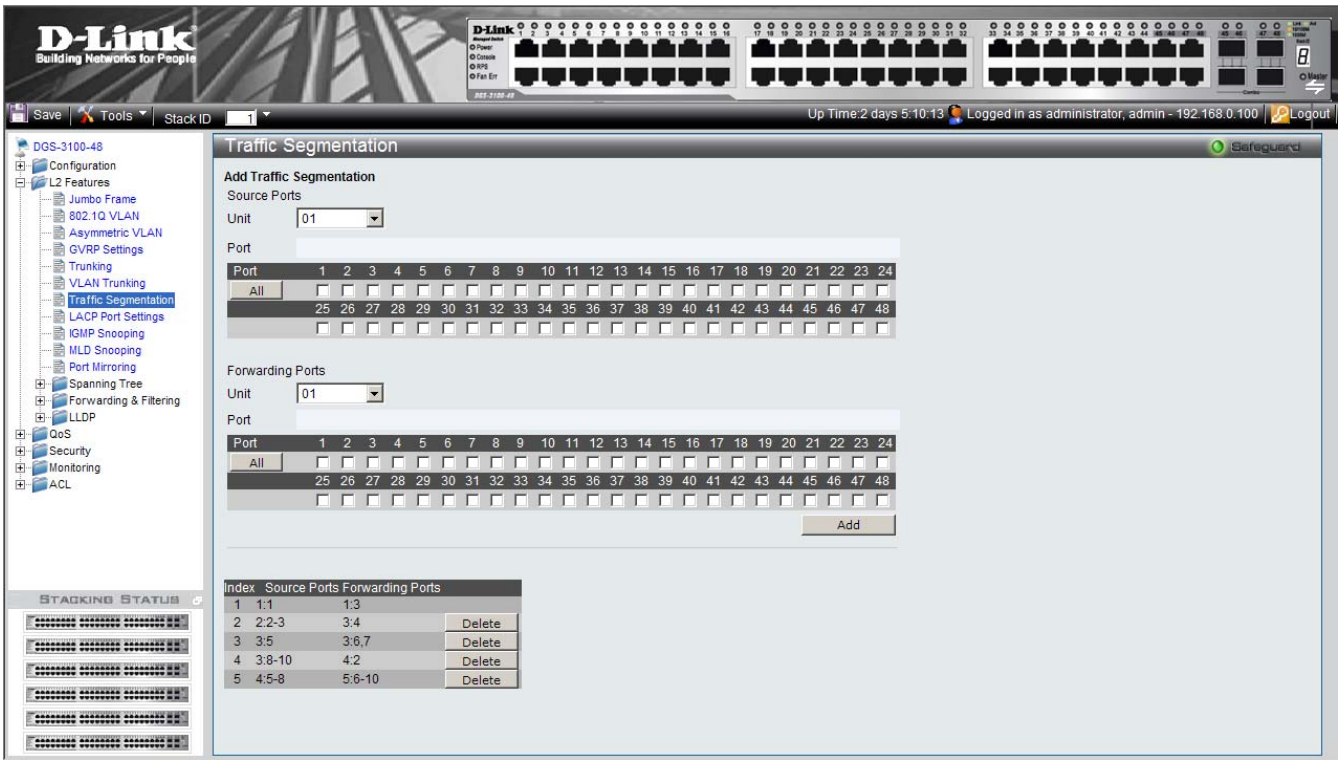


Figure 0–13 Traffic Segmentation Page

The Traffic Segmentation Page contains the following fields:

Field	Description
Source Ports	The port(s) from which the traffic is forwarded by the forwarding port(s). *Unit* or *LAG* — The stacking member's Unit ID and LAGs on which the source port is located. *Port* — The source port number.
Forwarding Ports	The port(s) from which the traffic from the source port is transmitted. *Unit* or *LAG* — The stacking member's Unit ID and LAGs on which the forwarding port is located. *Port* — The forwarding port number.

2. Define the Source and Forwarding Ports.
3. Click Add. The new traffic forwarding definition appears in the Traffic Segmentation table, and the device is updated.

To delete a Traffic Segmentation entry:

4. Select the entry in the table.
5. Click Delete. The entry is deleted, and the device is updated.

Configuring LACP

LAG ports can contain different media types if the ports are operating at the same speed. Aggregated links can be set up manually or automatically established by enabling LACP on the relevant links. Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed. The *LACP Port Settings Page* contains fields for configuring LACP LAGs.

1. Click **L2 features > LACP Port Settings**. The *LACP Port Settings Page* opens:

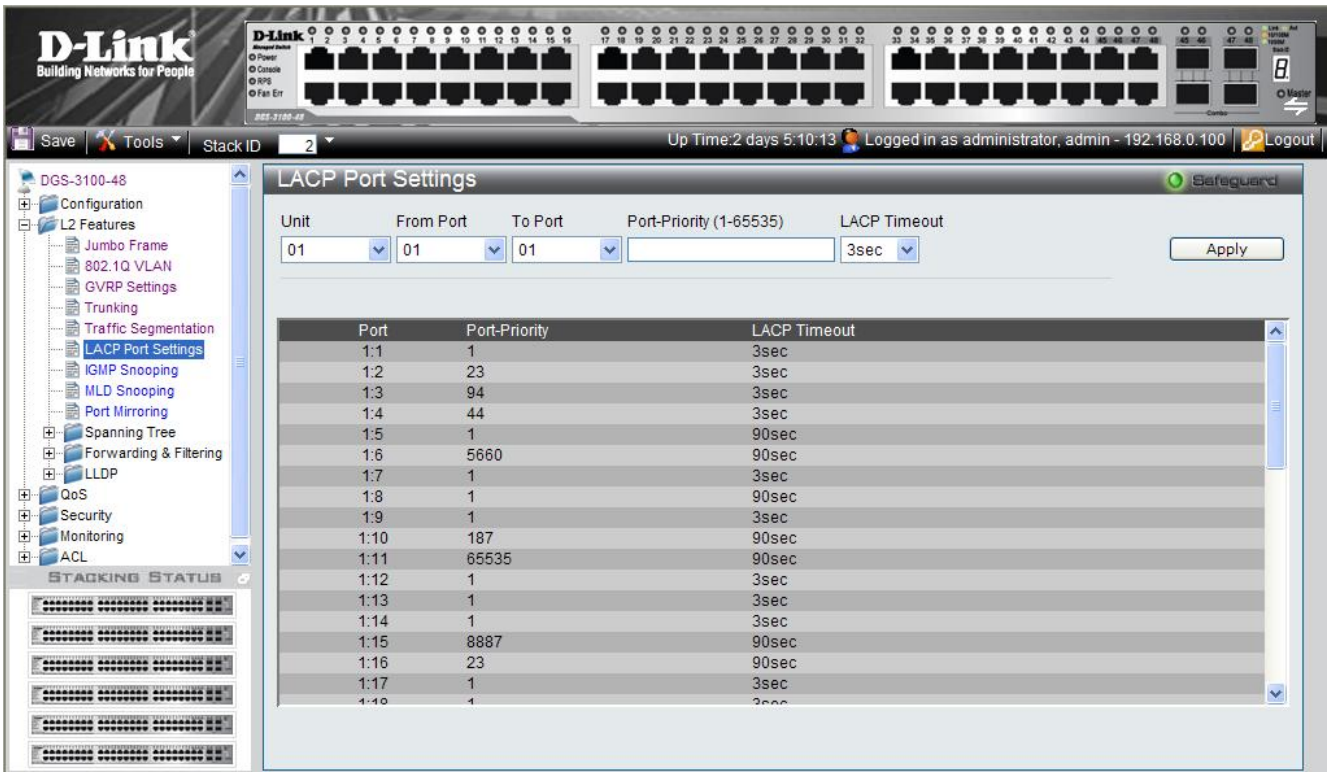


Figure 0–14 LACP Port Settings Page

The LACP Port Settings Page contains the following fields:

Field	Description
Unit	Defines the stacking member's Unit ID for which LACP parameters are displayed.
From Port	Defines the first port number that is displayed to which timeout and priority values are assigned.
To Port	Defines the last port number that is displayed to which timeout and priority values are assigned.
Port-Priority (1-65535)	Displays the LACP priority value for the port. The field range is 1-65535.
Timeout	Defines the administrative LACP timeout. The possible field values are: *Short (3 Sec)* — Defines the LACP timeout as 3 seconds. *Long (90 Sec)* — Defines the LACP timeout as 90 seconds. (This is the default value).

2. Select a stacking member in the *Unit* field.
3. Select the ports to and from which the LACP parameters are displayed in the *From/To Port* fields.
4. Define the Port-Priority and LACP Timeout fields.
5. Click Apply. The LACP parameters are defined, and the device is updated.

Defining IGMP Snooping

When IGMP Snooping is enabled globally, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets and determines the following information:

- Which ports want to join which Multicast groups.
- Which ports have Multicast routers generating IGMP queries.
- Which routing protocols are forwarding packets and Multicast traffic.

Ports requesting to join a specific Multicast group issue an IGMP report, specifying that this Multicast group is accepting members. This results in the creation of the Multicast filtering database.

IGMP Snooping configuration page supports also IGMP Querier.

1. Click **L2 Features > IGMP Snooping**. The *IGMP Snooping Page* opens:

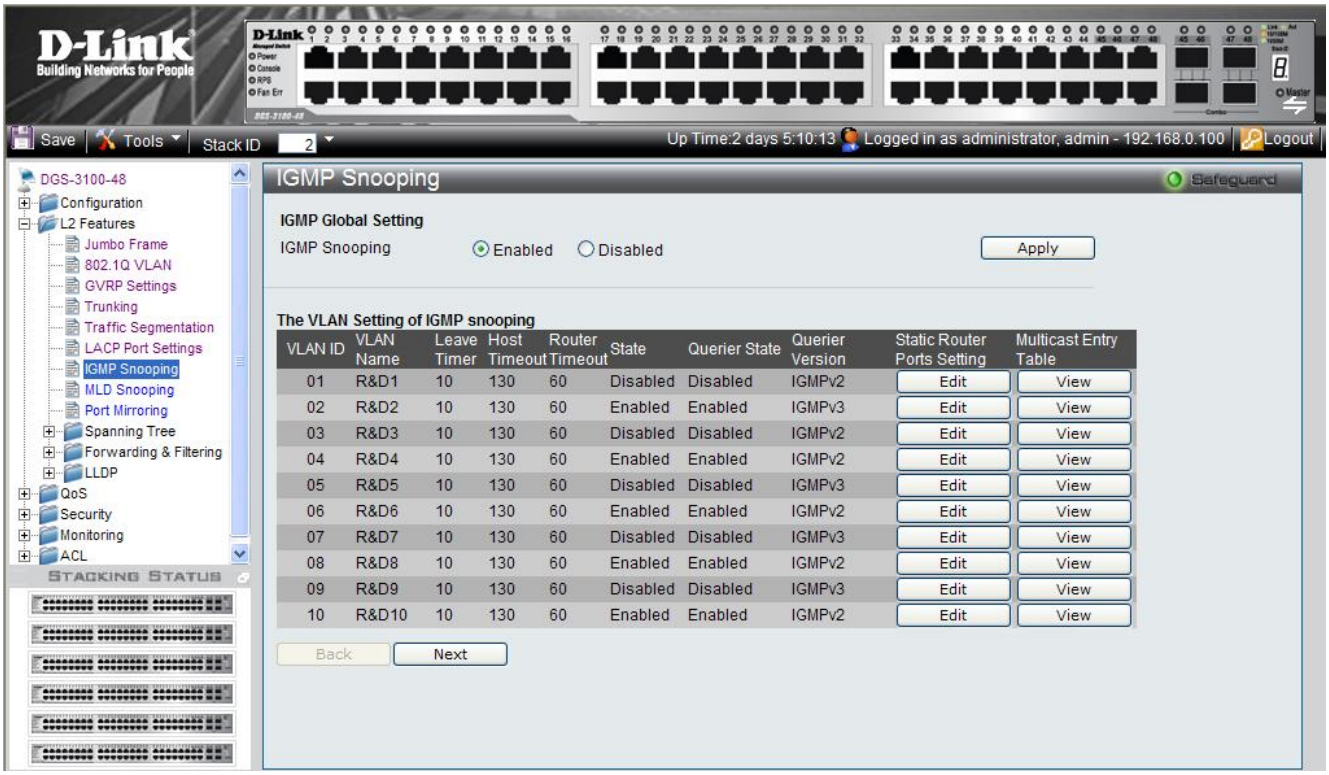

D-Link
Building Networks for People
Save
Tools
Stack ID
2
Up Time:2 days 5:10:13
Logged in as administrator, admin - 192.168.0.100
Logout
DGS-3100-48
Configuration
L2 Features
Jumbo Frame
802.1Q VLAN
GVRP Settings
Trunking
Traffic Segmentation
LACP Port Settings
IGMP Snooping
MLD Snooping
Port Mirroring
Spanning Tree
Forwarding & Filtering
LLDP
QoS
Security
Monitoring
ACL
STACKING STATUS
IGMP Snooping
Safeguard
IGMP Global Setting
IGMP Snooping
Enabled
Disabled
Apply
The VLAN Setting of IGMP snooping
VLAN ID | VLAN Name | Leave Timer | Host Timeout | Router Timeout | State | Querier State | Querier Version | Static Router Ports Setting | Multicast Entry Table
01 | R&D1 | 10 | 130 | 60 | Disabled | Disabled | IGMPv2 | Edit | View
02 | R&D2 | 10 | 130 | 60 | Enabled | Enabled | IGMPv3 | Edit | View
03 | R&D3 | 10 | 130 | 60 | Disabled | Disabled | IGMPv2 | Edit | View
04 | R&D4 | 10 | 130 | 60 | Enabled | Enabled | IGMPv2 | Edit | View
05 | R&D5 | 10 | 130 | 60 | Disabled | Disabled | IGMPv3 | Edit | View
06 | R&D6 | 10 | 130 | 60 | Enabled | Enabled | IGMPv2 | Edit | View
07 | R&D7 | 10 | 130 | 60 | Disabled | Disabled | IGMPv3 | Edit | View
08 | R&D8 | 10 | 130 | 60 | Enabled | Enabled | IGMPv2 | Edit | View
09 | R&D9 | 10 | 130 | 60 | Disabled | Disabled | IGMPv3 | Edit | View
10 | R&D10 | 10 | 130 | 60 | Enabled | Enabled | IGMPv2 | Edit | View
Back
Next

Figure 0–15 IGMP Snooping Page

The IGMP Snooping Page contains the following fields:

Field	Description
IGMP Snooping	Enables or disables IGMP Snooping. Bridge Multicast Filtering must first be enabled in order to enable IGMP Snooping. The possible field values are: *Enabled* — Enables IGMP Snooping on the device. *Disabled* — Disables IGMP Snooping on the device. (This is the default value).
VLAN ID	Specifies the VLAN ID.
VLAN Name	Displays the user-defined VLAN name.
Leave Timer	Defines the time a host waits to receive a Join message from another station after requesting to leave the IGMP group, prior to timing out. If a Leave Timeout occurs, the switch notifies the Multicast device to stop sending traffic. The Leave Timeout value is either user-defined, or an immediate leave value. The default timeout is 10 seconds. The field range is 0-16711450 seconds.

Field	Description
Host Timeout	Defines the time the host waits to receive a message before timing out. The default time is 260 seconds. The field range is 60-16711450 seconds.
Router Timeout	Defines the time the Multicast router waits to receive a message before it times out. The default value is 300 seconds. The field range is 1-16711450 seconds.
State	Indicates if IGMP snooping is enabled on the VLAN. The possible field values are: *Enable* — Enables IGMP Snooping on the VLAN. *Disable* — Disables IGMP Snooping on the VLAN. (This is the default value).
Querier State	Indicates if an IGMP Querier is enabled on the VLAN. The possible field values are: *Enabled* — An IGMP Querier is enabled on the VLAN. *Disabled* — An IGMP Querier is disabled on the VLAN. (This is the default value).
Querier Version	Indicates the IGMP Querier version on the VLAN. The possible field values are IGMPv2 and IGMPv3 (The default is IGMPv2).
Static Router Port Setting (Edit button)	Displays the IGMP Snooping and Static Router Ports Settings Page.
Multicast Entry Table (View Button)	Displays the Multicast Entry Table.

2. Click Edit. The *IGMP Snooping and Static Router* Ports Settings Page opens:

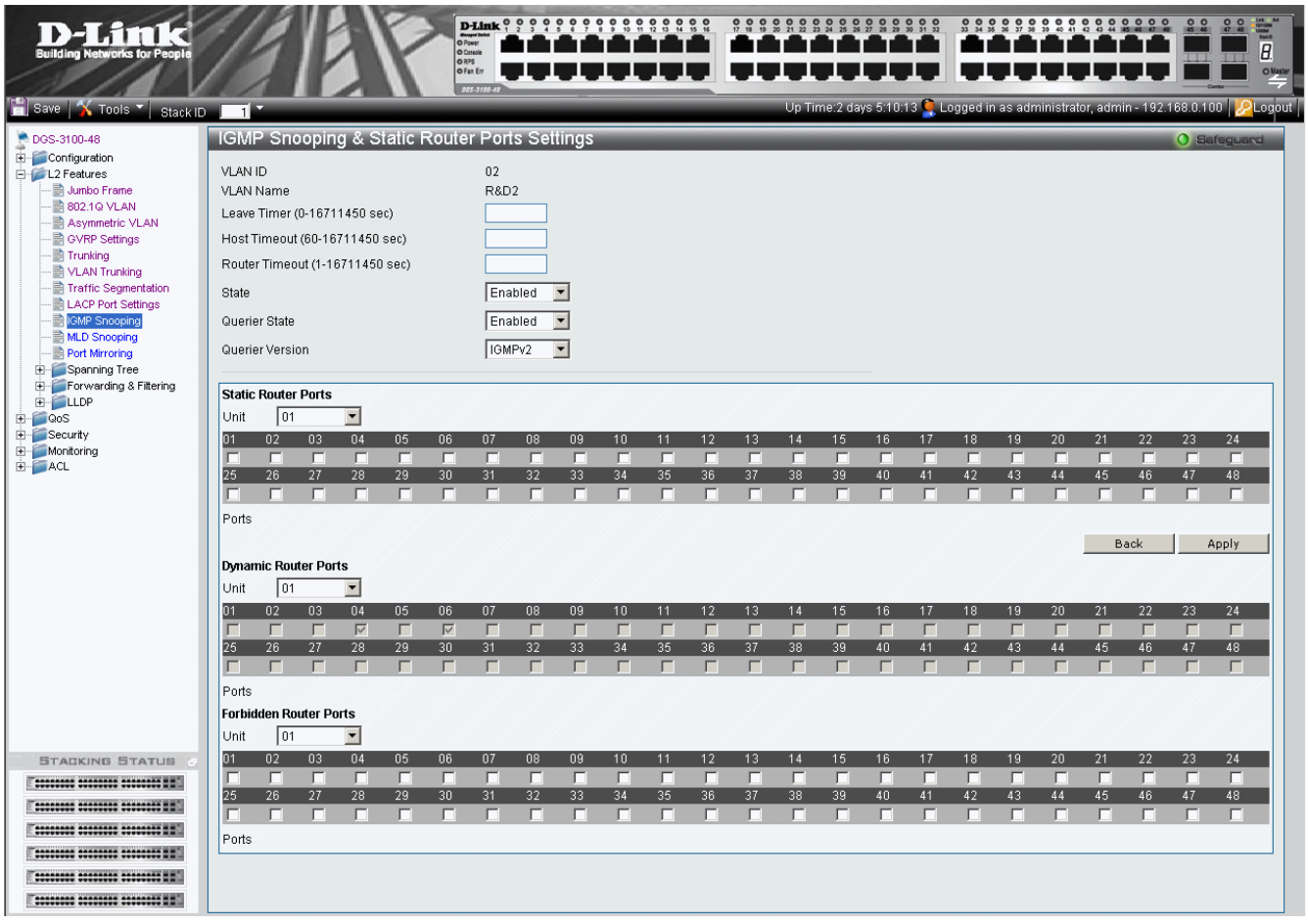


Figure 0–16 IGMP Snooping and Static Router Ports Settings Page

The IGMP Snooping and Static Router Ports Settings Page contains the following fields:

Field	Description
VLAN ID	Specifies the VLAN ID
VLAN Name	Displays the user-defined VLAN name.
Leave Timer	Defines the time a host waits to receive a Join message from another station after requesting to leave the IGMP group, prior to timing out. If a Leave Timeout occurs, the switch notifies the Multicast device to stop sending traffic The Leave Timeout value is either user-defined, or an immediate leave value. The default timeout is 10 seconds. The field range is 0-16711450 seconds.
Host Timeout	Defines the time the host waits to receive a message before timing out. The default time is 260 seconds. The field range is 60-16711450 seconds.
Router Timeout	Defines the time the Multicast router waits to receive a message before it times out. The default value is 300 seconds. The field range is 1-16711450 seconds.
State	Indicates if IGMP snooping is enabled on the VLAN. The possible field values are: *Enable* — Enables IGMP Snooping on the VLAN. *Disable* — Disables IGMP Snooping on the VLAN
Querier State	Defines the IGMP Querier status on the VLAN. The possible field values are: *Enabled* — Enables an IGMP Querier on the VLAN. *Disabled* — Disables an IGMP Querier on the VLAN..
Querier Version	Defines the IGMP Querier version on the VLAN. The possible field values are IGMPv2 and IGMPv3.
Unit	Defines the unit number.
Static Router Ports	Defines the port numbers which can be added as static router ports.
Ports	Indicates the units and allocated ports as static router ports.
Dynamic Router Ports	Displays the port numbers which was learned as dynamic router ports.
Forbidden Router Ports	Defines the ports to be added as forbidden router ports.
Ports	Indicates the units and port numbers defined as forbidden router ports.

3. Define the Leave Timer, Host Timeout, Router Timeout, State, Querier State, Querier Version, Static Dynamic and Forbidden Router Ports fields.
4. Click Apply. IGMP Snooping and Static Router Port Settings are defined, and the device is updated.

Defining MLD Snooping

Multicast Listener Discovery (MLD) Snooping performs the same function for IPv6 multicast routers as IGMP Snooping does for IPv4 multicast routers.

The device supports two versions of MLD Snooping:

- MLDv1 Snooping detects MLDv1 control packets and sets up traffic bridging based on IPv6 destination multicast addresses. MLDv1 is equivalent to IGMPv2.
- MLDv2 Snooping uses control packets to set up traffic forwarding based on source IPv6 address and destination IPv6 multicast address. MLDv2 is equivalent to IGMPv3.

In a similar approach to IGMP snooping, MLD frames are snooped as they are forwarded by the switch from stations to an upstream multicast router. This facility allows a switch to determine the following:

- Where (on which ports) stations interested in joining a specific multicast group are located
- Where (on which ports) multicast routers sending multicast frames are located

This knowledge is used to exclude irrelevant ports (ports for which no stations have registered to receive a specific multicast group) from the forwarding set of an incoming multicast frame.

Two port types can be defined in the system:

- Host port - a port connected to an end-node device running an IGMP/MLD (multicast communication) application.
- Multicast Router (mrouter) port - a port connecting multicast router ports to the switch. This port receives all IGMP/MLD control packets (reports and queries) as well as all multicast data traffic associated with dynamic Multicast groups.

A port can be both a host port and mrouter port simultaneously.

1. Click **L2 Features > MLD Snooping**. The *MLD Snooping Page* opens:

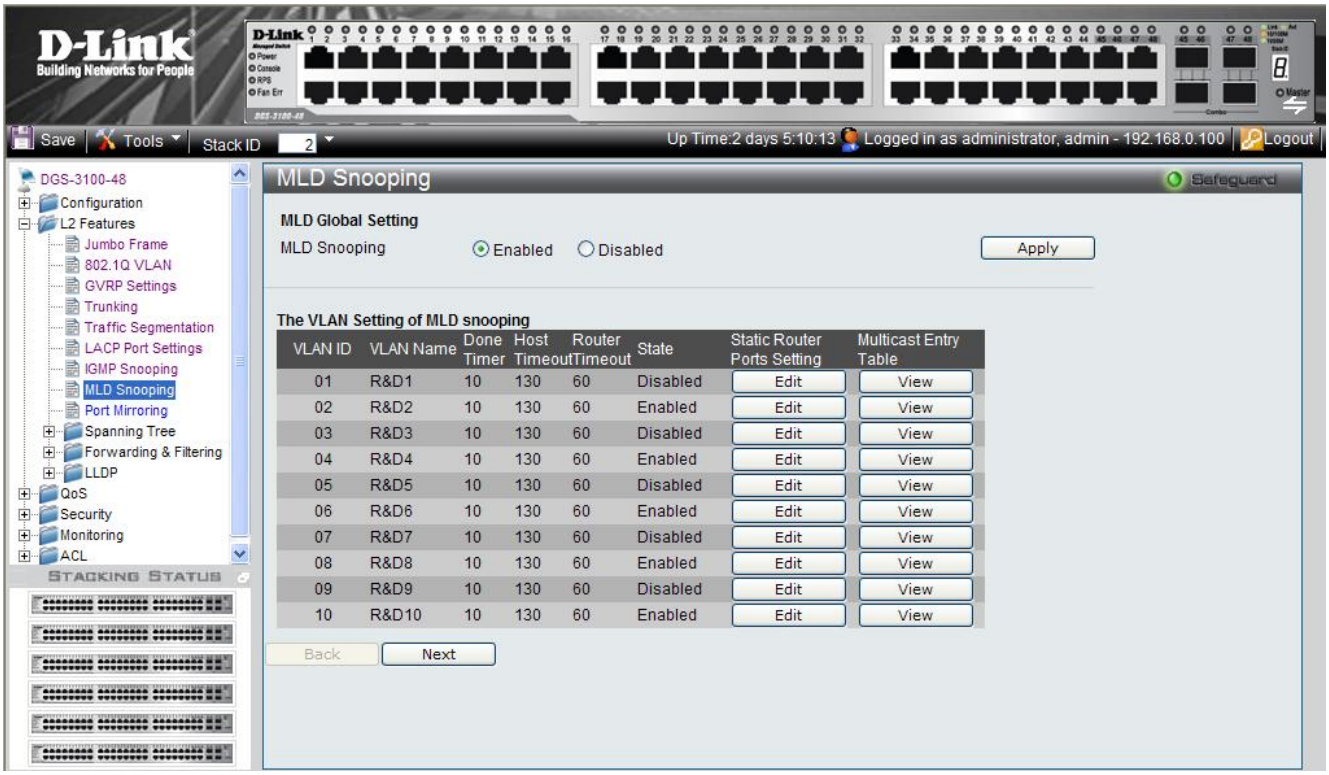


Figure 0–17 MLD Snooping Page

The MLD Snooping Page contains the following fields:

Field	Description
MLD Snooping	Enables or disables MLD Snooping. The possible field values are: *Enabled* — Enables MLD Snooping on the device. *Disabled* — Disables MLD Snooping on the device. (This is the default value).
VLAN ID	Specifies the VLAN ID.
VLAN Name	Displays the user-defined VLAN name.
Done Timer	Specifies the time interval in seconds after which a port is removed from the Multicast membership group. Ports are removed from the Multicast membership when the port sends a Done Message, indicating the port requests to leave the Multicast group. The field range is 0-16711450 seconds. The default timeout is 10 seconds.
Host Timeout	Specifies the time interval in seconds after which a port is removed from a Multicast Group. Ports are removed if a Multicast group MLD report was not received from a Multicast port within the defined *Host Timeout* period. The possible field range is 60 - 16711450 seconds. The default timeout is 260 seconds.
Router Timeout	Specifies the time interval in seconds the Multicast router waits to receive a message before it times out. The possible field range is 60 - 16711450 seconds. The default timeout is 300 seconds.
State	Indicates if MLD snooping is enabled on the VLAN. The possible field values are: *Enabled* —MLD Snooping is enabled on the VLAN. *Disable*d —MLD Snooping is disabled on the VLAN. (This is the default value).
Static Router Port Setting (Edit button)	Displays the MLD Snooping & Static Router Ports Settings Page.
Multicast Entry Table (View Button)	Displays the Multicast Entry Table.

2. Click Edit. The *MLD Snooping & Static Router Ports Settings Page* opens:

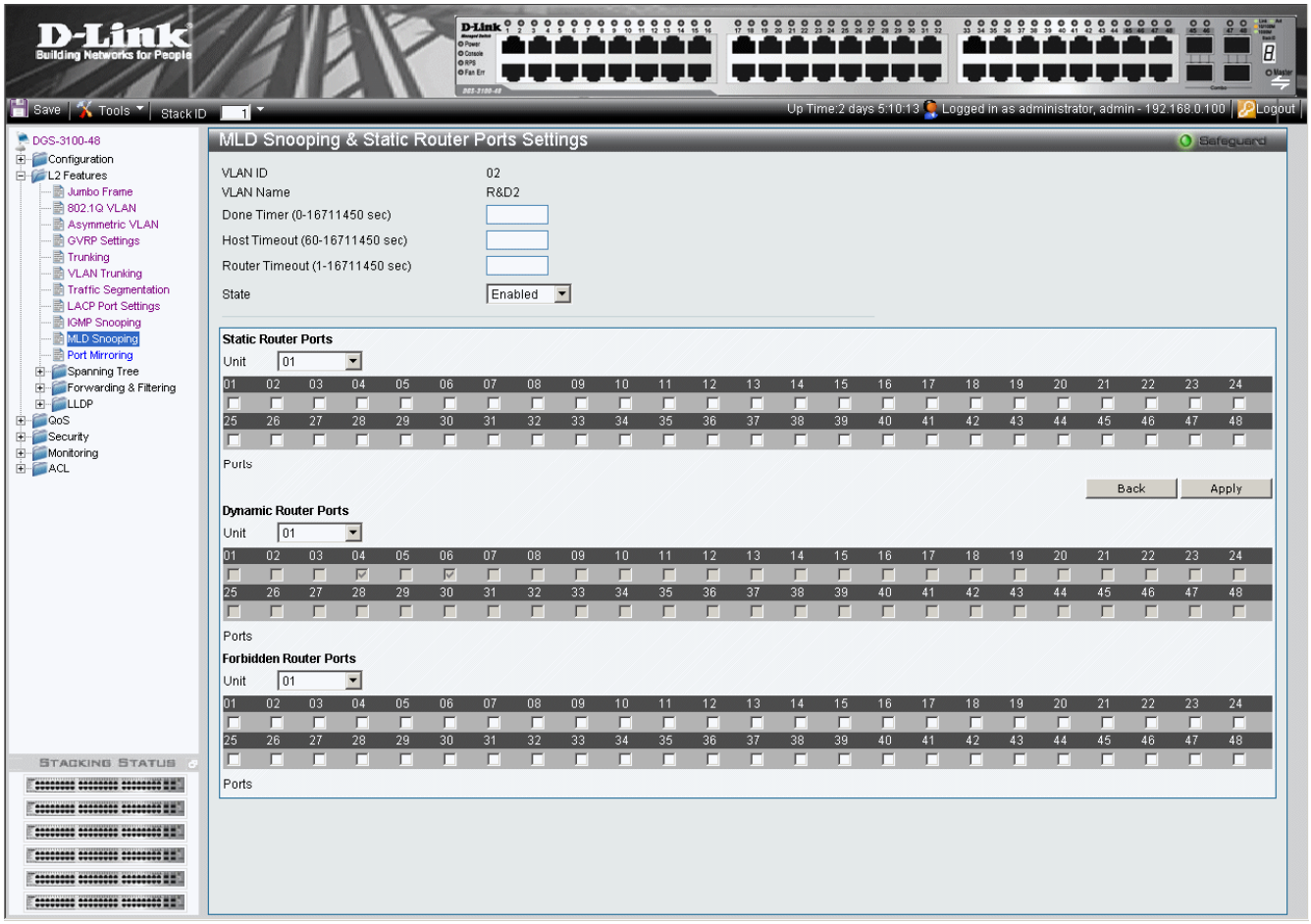


Figure 0–18 MLD Snooping & Static Router Ports Settings Page

The MLD Snooping & Static Router Ports Settings Page contains the following fields:

Field	Description
VLAN ID	Specifies the VLAN ID
VLAN Name	Displays the user-defined VLAN name.
Done Timer (0-16711450 sec)	Defines the time interval in seconds after which a port is removed from the Multicast membership group. Ports are removed from the Multicast membership when the port sends a Done Message, indicating the port requests to leave the Multicast group. The field range is 0 - 16711450 seconds. The default timeout is 10 seconds.
Host Timeout (60-16711450 sec)	Defines the time interval in seconds after which a port is removed from a Multicast Group. Ports are removed if a Multicast group MLD report was not received from a Multicast port within the defined *Host Timeout* period. The possible field range is 60 - 16711450 seconds. The default timeout is 260 seconds.
Router Timeout (1-16711450 sec)	Defines the time interval in seconds the Multicast router waits to receive a message before it times out. The possible field range is 1 - 16711450 seconds. The default timeout is 300 seconds.
State	Indicates if MLD snooping is enabled on the VLAN. The possible field values are: *Enable* — Enables MLD Snooping on the VLAN. *Disable* — Disables MLD Snooping on the VLAN
Unit	Defines the unit number.

Field	Description
Static Router Ports	Defines the port numbers in the selected unit to be added as static router ports.
Ports	Displays the unit:port numbers defined as static router ports.
Dynamic Router Ports	Displays the port numbers in the selected unit learned as dynamic router ports.
Ports	Displays the unit:port numbers defined as dynamic router ports.
Forbidden Router Ports	Defines the port numbers in the selected unit to be added as forbidden router ports.
Ports	Displays the unit:port numbers defined as forbidden router ports.

3. Define the Done Timer, Host Timeout, Router Timeout, State, Static, Dynamic, and Forbidden Router Ports fields.
4. Click Apply. MLD Snooping and Static Router Port Settings are defined, and the device is updated.

Configuring Port Mirroring

Switches inherently forward frames to relevant ports only. This creates difficulty when traffic needs to be monitored, either for information gathering (such as statistical analysis, security traces, etc.) or for troubleshooting higher-layer protocol operation. The device supports up to 8 source ports.

To enable the use of traffic analysis and monitoring devices, it is recommended enabling the user to specify that a desired 'target' port receives a copy of all traffic passing through a designated 'source' port. All ports can be designated as source ports.

In order to activate Port Mirroring, the target port must belong to the default VLAN.

1. Click **L2 Features > Port Mirroring**. The *Port Mirroring Page* opens:

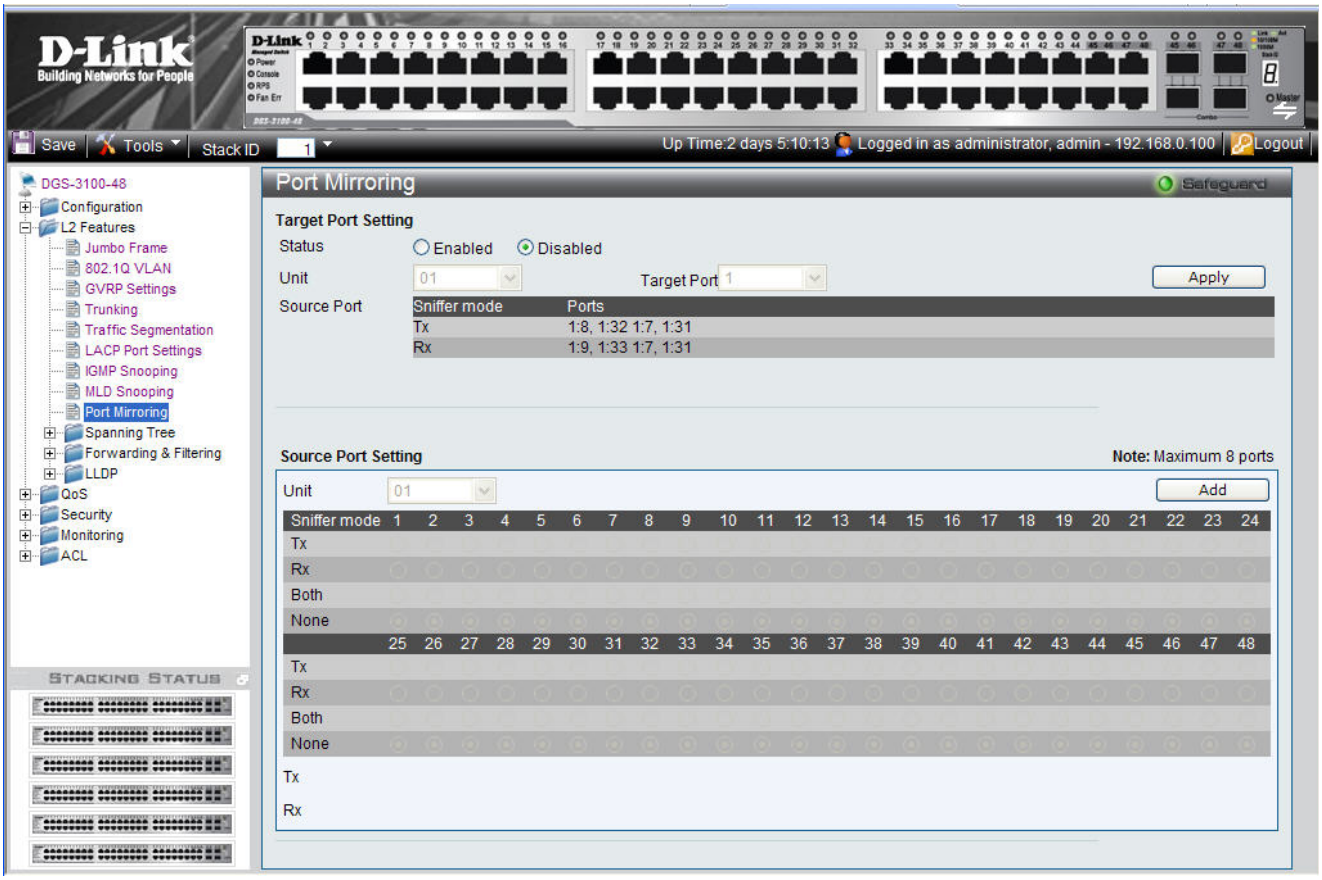


Figure 0–19 Port Mirroring Page

The Port Mirroring Page contains the following fields:

Field	Description
Status	Enables or disables target port setting. The default is Disabled.
Unit	Defines the unit number.
Target Port	Defines the target port.
Source Port	Displays the Sniffer Mode and the source port.

Source Port Setting

Field	Description
Unit	Selects the Unit to be displayed.
Tx	Indicates the transmit stream of data on the port.
Rx	Indicates the receive stream of data on the port.

Field	Description
Both	Defines the port mirroring on both receiving and transmitting ports.
None	Defines that port mirroring is not applied to the ports.

2. Define the *Status*, *Unit*, and *Target* fields.
3. Click Apply to activate the Port Mirroring function.
4. Define the *Unit*, *Tx*, and *Rx*. fields under Source Port Setting.
5. Click Add to capture the configured Source Ports in order to display them in the Source Port Setting table.

Configuring Spanning Tree

Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges, as well as providing a single path between end stations on a network, thus eliminating loops.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

The device supports the following STP versions:

Version	Description
Classic STP	Provides a single path between end stations, preventing loops from occurring.
Rapid STP	Detects and uses network topologies that provide faster convergence of the spanning tree, without creating forwarding loops.
Multiple STP	Provides various load balancing scenarios. For example, if port A is blocked in one STP instance, the same port can be placed in Forwarding State in another STP instance.

The *STP Bridge Global Settings Page* contains parameters for enabling STP on the device. This section contains the following topics:

- Defining Spanning Tree Global Parameters
- Defining STP Port Settings
- Defining Multiple Spanning Tree Configuration Identification
- Defining MSTP Port Information

Defining Spanning Tree Global Parameters

While Classic STP prevents Layer 2 forwarding loops in a general network topology, convergence can take between 30-60 seconds. This time may delay detecting possible loops and propagating status topology changes. Rapid Spanning Tree Protocol (RSTP) detects and uses network topologies that allow a faster STP convergence without creating forwarding loops.

When STP is enabled, Loopback Detection (LBD) is also enabled. Loopback Detection identifies any Loopback BPDUs that the Spanning Tree application receives on a port. In this case, the device sends a Loopback Detection trap for the port. When the condition is resolved, the device sends a Loopback Detection Resolved trap and the port learns the STP configuration again.

The STP Bridge Global Settings Page contains parameters for enabling STP on the device.

1. Click **L2 Features > Spanning Tree > STP Bridge Global Settings**. The *STP Bridge Global Settings Page* opens:

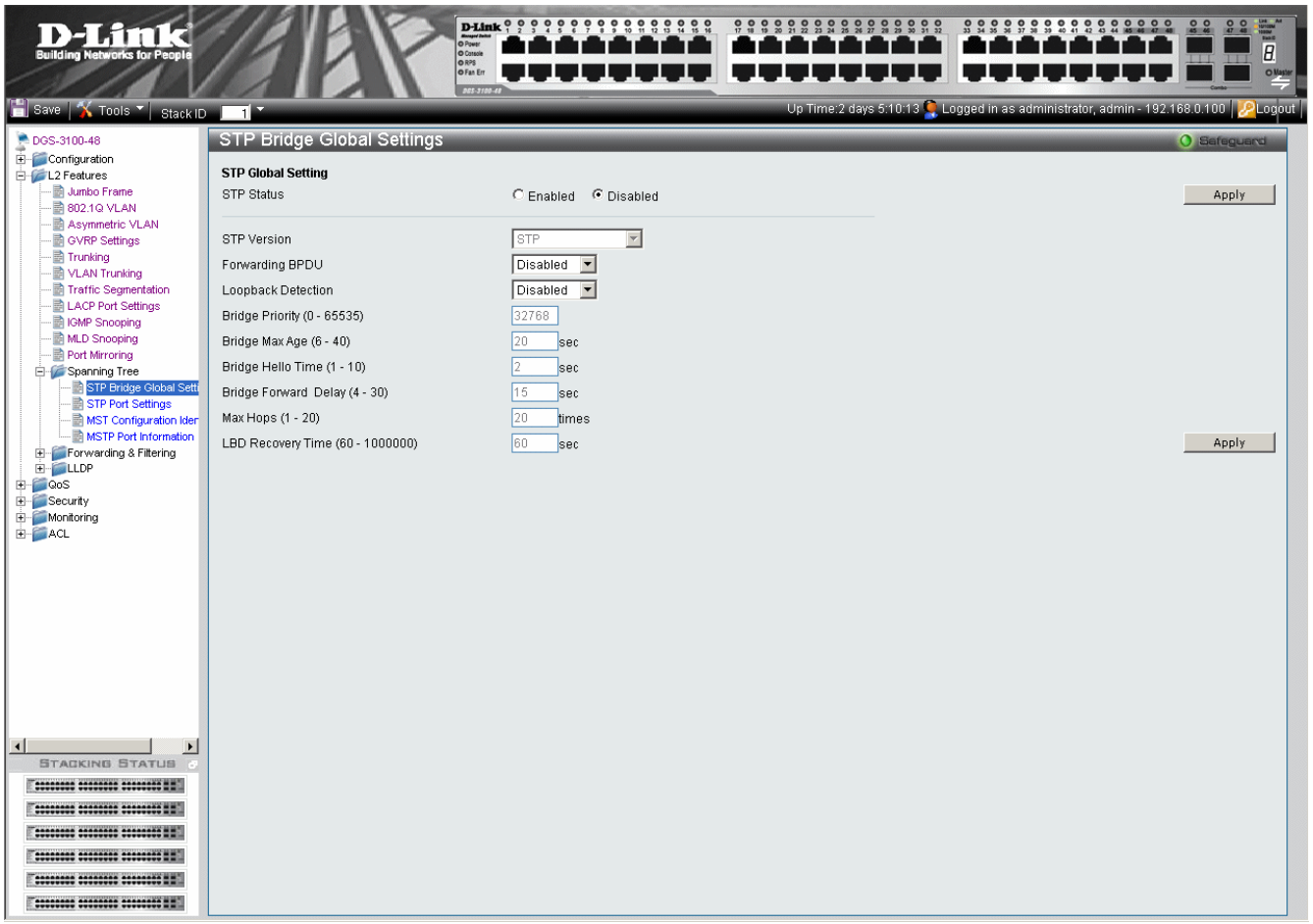


Figure 0–20 STP Bridge Global Settings Page

The STP Bridge Global Settings Page contains the following fields:

Field	Description
STP Status	Enable or disables STP globally on the switch. The default is Disabled.
STP Version	Defines the desired version of STP to be implemented on the switch. There are three choices: *STP* — Sets the Spanning Tree Protocol (STP) globally on the switch. *RSTP* — Sets the Rapid Spanning Tree Protocol (RSTP) globally on the switch. *MSTP* — Sets the Multiple Spanning Tree Protocol (MSTP) globally on the switch.
Forwarding BPDU	Bridges use Bridge Protocol Data Units (BPDU) to provide spanning tree information. STP BPDUs filtering is useful when a bridge interconnects two regions; each region needing a separate spanning tree. BPDU filtering functions only when STP is disabled

Field	Description
	either globally or on a single interface. The possible values are: *Enabled* – Allows the forwarding of STP BPDU packets from other network devices.. *Disabled* – BPDU forwarding is disabled on the device. (This is the default value)
Bridge Priority (0 – 65535)	Specifies the selected spanning tree instance device priority. The field range is 0-65535. The default value is 32768.
Bridge Max Age (6- 40)	Set to ensure old information is not circulated endlessly through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value aids in determining that the switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user can choose between 6 and 40 seconds. The default value is 20.
Bridge Hello Time (1 – 10)	The interval between two transmissions of BPDU packets sent by the Root Bridge to indicate to all other switches that it is indeed the Root Bridge. The default value is 2.
Bridge Forward Delay (4 – 30)	Defines the time any port on the switch is in the listening state while moving from the blocking state to learning state and then to the forwarding state. The default value is 15.
Max Hops (1 – 20)	Specifies the total number of hops that occur before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out. The possible field range is 1-20. The field default is 20 hops.
LBD Recovery Time (30 – 86400)	Defines the amount of time that passes after ports that were shut down through LBD are moved to active The possible field range is 30 - 86400 seconds. The default is 60 seconds (2 minutes).

2. Select Enable/Disable in the *STP* Status field.
3. Define the STP Version, Forwarding BPDU, Bridge Priority, Bridge Max Age, Bridge Hello Time, Bridge Forward Delay, Max Hops fields and LBD Recovery Time.
4. Click Apply. The Spanning Tree Global Parameters are defined, and the device is updated.

NOTE: The Global STP status default was 'Enable' in previous software versions and was changed to 'Disable'. Please note that if STP enabled is the required state, you should enable STP via the WEB GUI or the CLI.

NOTE: In case of STP loopback the port will be shutdown, the port will be activated after the loopback is removed.

Defining STP Port Settings

STP can be set up on a port per port basis. In addition to setting Spanning Tree parameters for use at the switch level, the switch enables configuring groups of ports, in which case each port-group has its own spanning tree and requires some of its own configuration settings. An STP group uses the switch level parameters entered above, with the addition of Port Priority and Port Cost.

An STP group spanning tree works in the same way as the switch level spanning tree, however the root bridge concept is replaced with a root port concept. A root port is a group port designated as the connection to the network for the group, based on port priority and port cost. Redundant links are blocked, just as redundant links are blocked at the switch level.

The switch level STP blocks redundant links between switches (and similar network devices). The port level STP blocks redundant links within an STP Group.

It is advisable to define an STP Group to correspond to a VLAN group of ports.

1. Click **L2 Features > Spanning Tree > STP Port Settings.** The *STP Port Settings Page* opens:

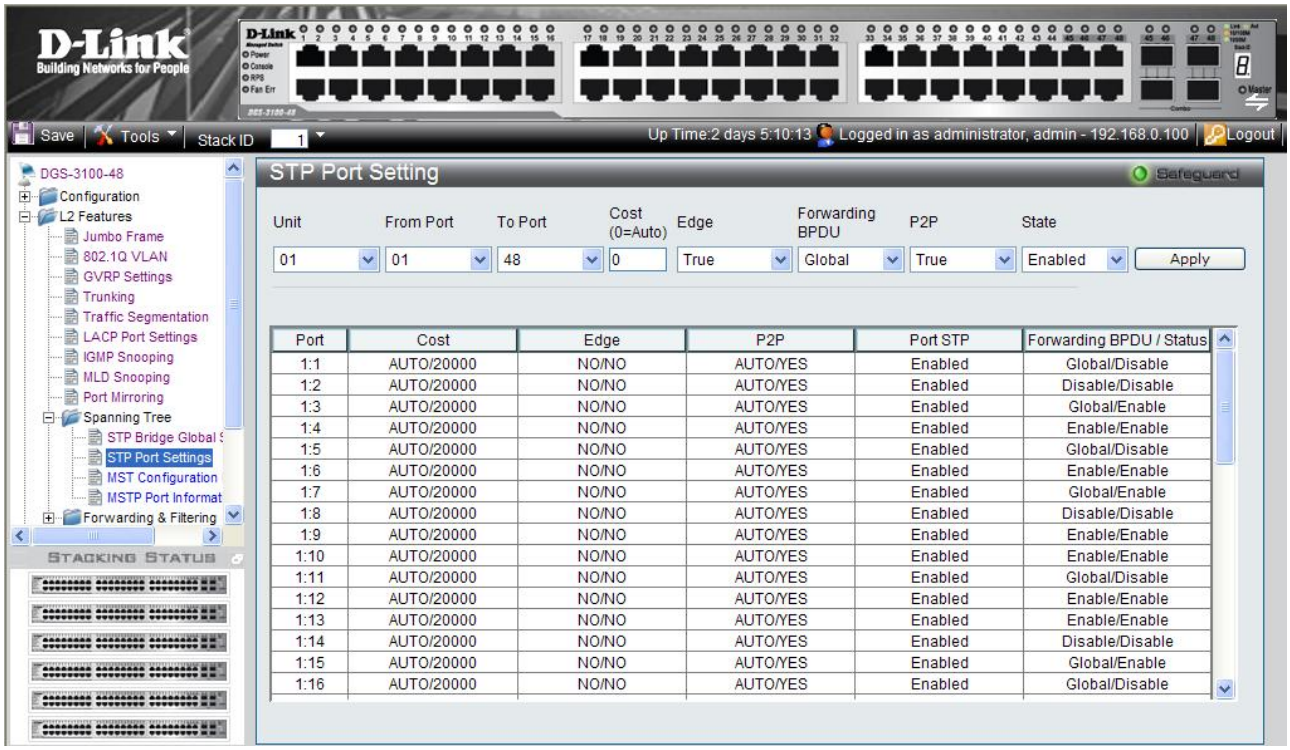


Figure 0–21 STP Port Settings Page

The STP Port Settings Page contains the following fields:

Field	Description
Unit	Indicates the stacking member for which the STP port settings are displayed.
From Port	Defines the first port in a consecutive sequence of ports.
To Port	Defines last port in a consecutive sequence of ports.
Cost (0=Auto)	Defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto). 0 (auto) — Setting 0 for the external cost automatically sets the speed for forwarding packets to the specified port(s) in the list (for optimal efficiency). Default port cost: 10Mbps port = 2000000, 100Mbps port = 200000. Gigabit port = 20000, Port-channel = 20000 Value 1-200000000 — Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.

Field	Description
Edge	Indicates whether the selected port is an edge port. The possible field values are: *True* — Defines the port as an edge port. Edge ports cannot create loops; however, they can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. *False* — Indicates that the port does not have edge port status.
Forwarding BPDU	Bridges use Bridge Protocol Data Units (BPDU) to provide spanning tree information. STP BPDUs filtering is useful when a bridge interconnects two regions; each region needing a separate spanning tree. BPDU filtering functions only when STP is disabled either globally or on a single interface. The possible field values are: *Disabled* – BPDU filtering is enabled on the port. *Enabled* – BPDU forwarding is enabled on the port (if STP is disabled). *Global* – BPDU filtering functions according to the device-wide setting (see *STP Bridge Global Settings Page*).
P2P	Indicates whether the P2P of selected port is enabled. The possible field values are: *True* — Indicates a point-to-point (P2P) link, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. *False* — Indicates that the port cannot have P2P status. *Auto* — Allows the port to have P2P status whenever possible and operate as if the P2P status were true. (A port that operates in full-duplex is assumed to be point-to-point, while a half-duplex port is considered as a shared port) If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the P2P status changes to operate as if the P2P value were False. The default setting is Auto.
State	Set to enable or disable STP for the selected group of ports. The default is Enabled. The port STP State overrides the STP Global State

2. Define the Unit, From Port, To Port, Cost, Edge, P2P, and State fields.
3. Click Apply. The STP Port Settings are defined, and the device is updated.

Defining Multiple Spanning Tree Configuration Identification

Multiple Spanning Tree (MSTP) provides various load balancing scenarios by allowing multiple VLANs to be mapped to a single spanning tree instance, providing multiple pathways across the network. For example, while port A is blocked in one STP instance, the same port can be placed in the Forwarding state in another STP instance.

The *MST Configuration Identification Page* contains information for defining global MSTP settings, including region names, MSTP revision level. To define MSTP:

1. Click **L2 Features > Spanning Tree > MST Configuration Identification**. The *MST Configuration Identification Page* opens:

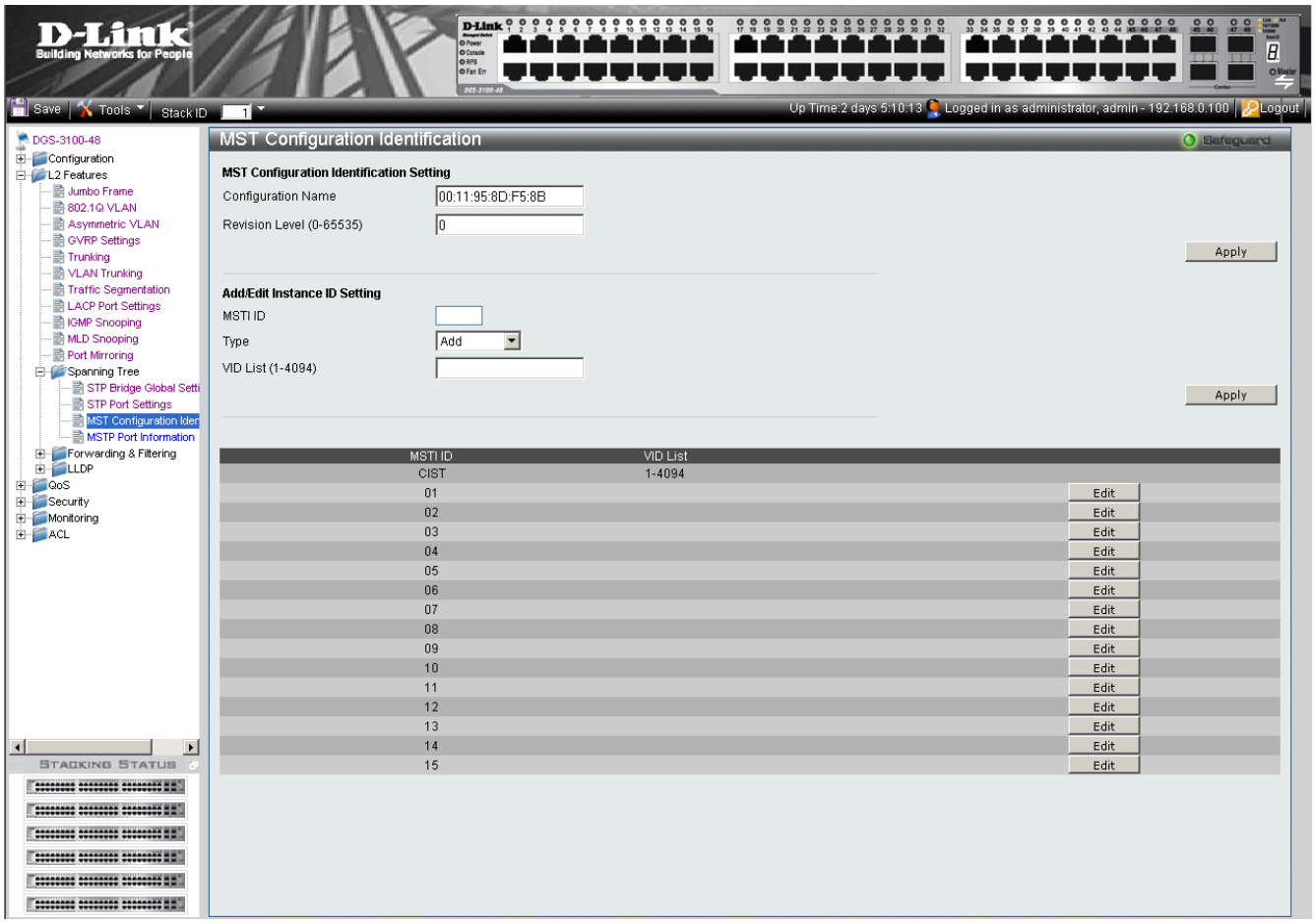


Figure 0–22 MST Configuration Identification Page

The MST Configuration Identification Page contains the following fields:

Field	Description
Configuration Name	A configured name set on the switch to uniquely identify the MSTI (multiple spanning tree instance). If a configuration name is not set, this field shows the MAC address of the device running MSTP.
Revision Level (0-65535)	This value, together with the configuration name, and identical vlans mapped for STP instance IDs identifies the MST region configured on the switch.
MSTI ID	Displays the MSTI ID associated with the VID List.
Type	Defines the type of edit. The possible values are: *Add* — Indicates that edit type is add *Remove* — Indicates that edit type is remove.
VID List (1-4094)	Displays the VID List.

2. Define the configuration name and revision level.
3. Click Apply.
4. Click Edit to an ID row to edit the ID value.
5. Define the new value.
6. Click Apply. The Multiple Spanning Tree Configuration Identification is defined, and the device is updated.

Defining MSTP Port Information

Network Administrators can assign MSTP Interface settings in the *MSTI Config Information Page*. To define MSTP interface settings:

1. **Click L2 Features > Spanning Tree > MSTP Port Information. The MSTI Config Information Page opens:**

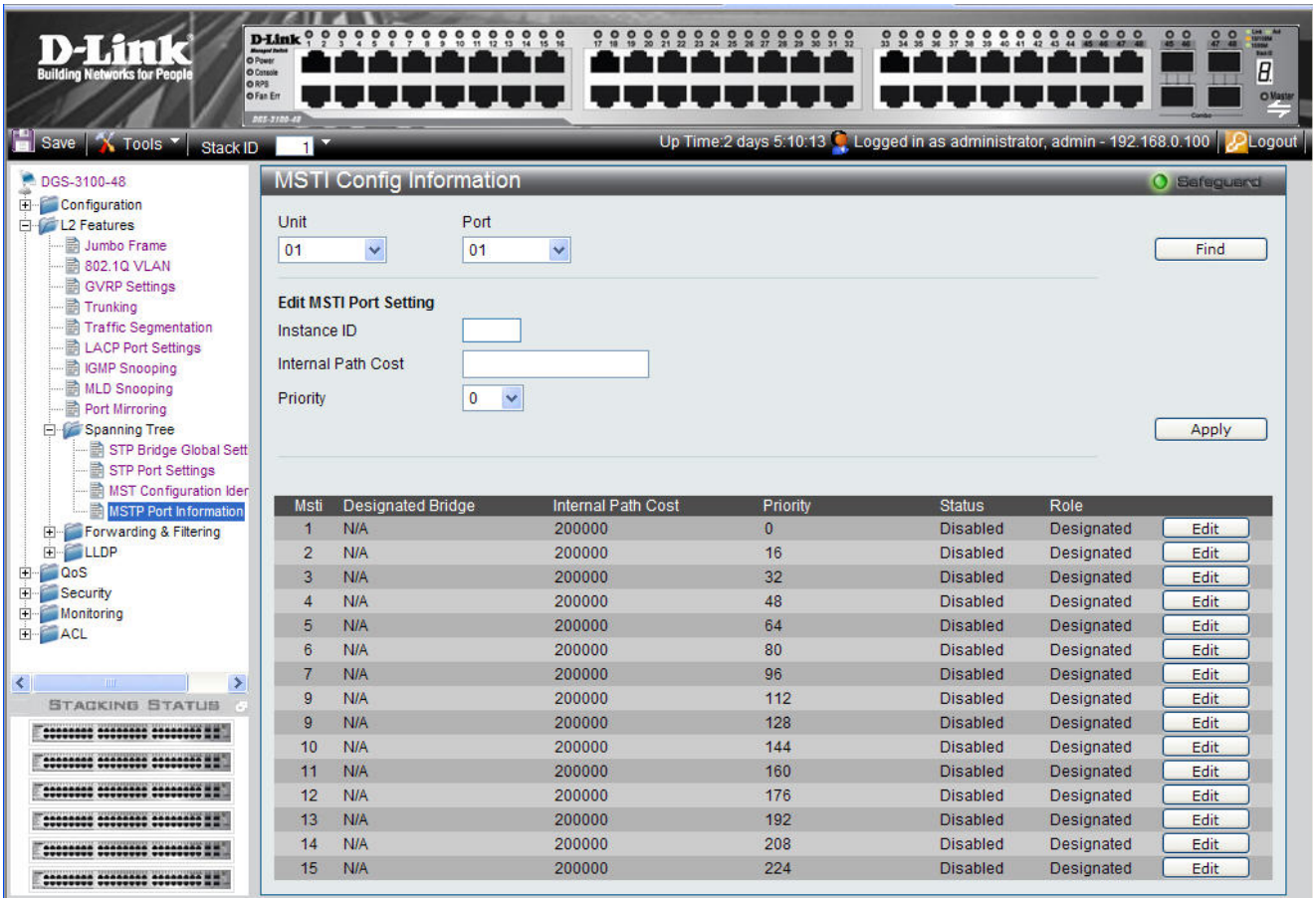


Figure 0–23 MSTI Config Information Page

The MSTI Config Information Page contains the following fields:

Field	Description
Unit	Defines the unit to find.
Port	Defines the Port to find.
Instance ID	Lists the MSTP instances configured on the device. Possible field range is 0-7.
Internal Path Cost	Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000. The default value is automatically set cost, according to its speed. Default port cost: 10Mbps port = 2000000, 100Mbps port = 200000. Gigabit port = 20000, Port-channel = 20000.

Field	Description
Priority	Defines the interface priority for the specified instance. The default value is 128.
Status	Indicates whether the port is enabled for the specific instance. The possible field values are: *Forwarding* — Enables the port for the specific instance. *Listening* - Processes BPDUs received from the system module *Learning* – Incorporates station location into its address database *Blocking* - Discards frames received from the attached segment and frames switched from another port for forwarding *Disabled* — Disables the port for the specific instance.
Role	Indicates the port role assigned by the STP algorithm to provide to STP paths. The possible field values are: *Enabled* — Enables the port for the specific instance. *Root* — Provides the lowest cost path to forward packets to the root device. *Designated* — Indicates the port or LAG through which the designated device is attached to the LAN. *Alternate* — Provides an alternate path to the root device from the root interface. *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link or when a LAN has two or more connections connected to a shared segment. *Disabled* — Indicates the port is not participating in the Spanning Tree.

2. Define the values in the *Unit* and *Port* fields.
3. Click Find.
4. Define the Internal Path Cost and Priority fields.
5. Click Apply.
6. Click Edit adjacent to an MSTI ID row to edit the values for Internal Path Cost and Priority.

Defining Forwarding and Filtering

This section contains information for configuring both Unicast and Multicast filtering, and contains the following topics:

- Defining Unicast Forwarding
- Defining Multicast Forwarding
- Defining Multicast Filtering
- Defining DLF Filtering

Defining Unicast Forwarding

The Unicast Forwarding Page contains parameters for configuring Unicast entries.

1. Click **L2 Features > Forward & Filtering > Unicast Forwarding**. The *Unicast Forwarding Page* opens**:**

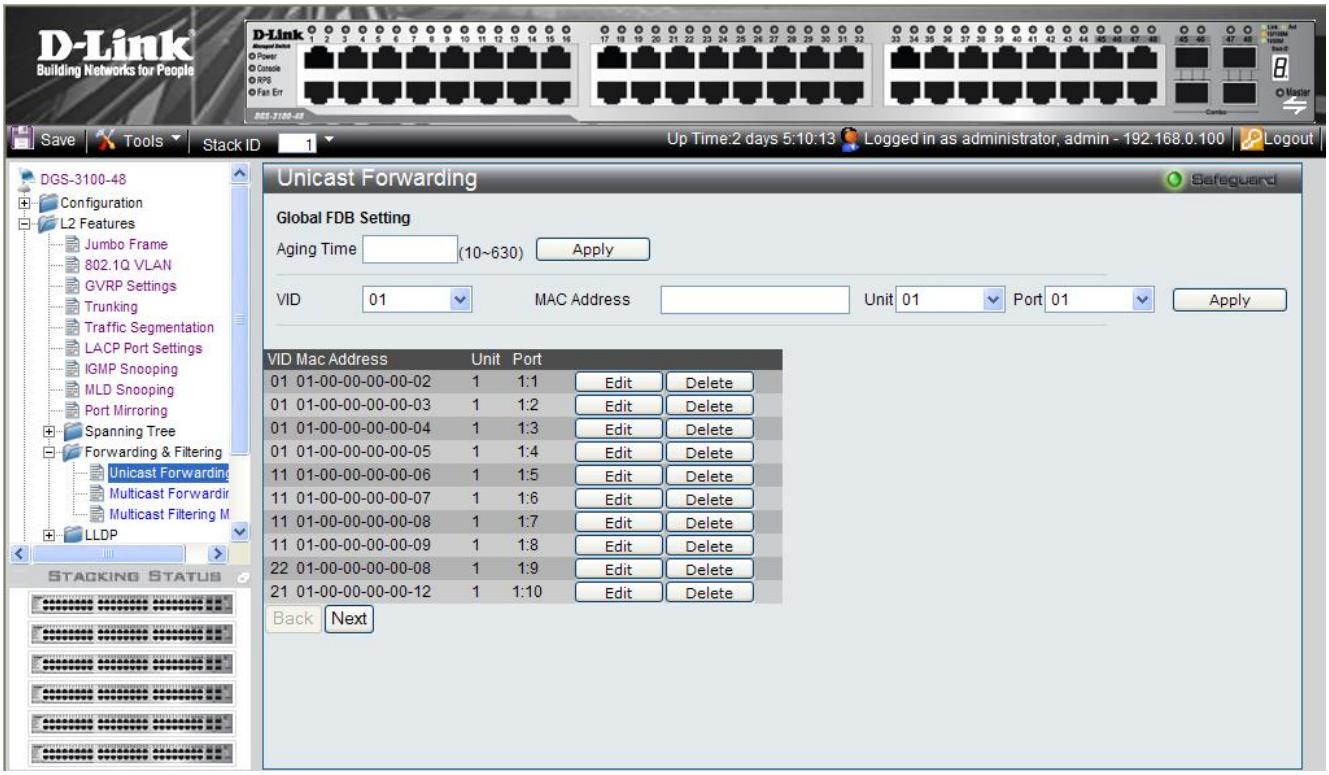


Figure 0–24 Unicast Forwarding Page

The Unicast Forwarding Page contains the following fields:

Field	Description
Aging Time	Defines the aging time of a Unicast packet. If the packet is not forwarded after this interval, it is discarded. Aging time is a global (FDB) database setting.
VID	Defines the VLAN ID.
MAC Address	Defines the Unicast MAC address to which packets are forwarded.
Unit	Defines the unit number.
Port	Defines the port number.

2. Define the VID, MAC Address, Unit, and Port fields.
3. Click Apply. The Unicast are defined, and the device is updated.

To edit a FDB table entry:

1. Select the entry.
2. Click Edit.
3. Define the values.
4. Click Apply. The entry is updated, and the device is updated.

To delete a FDB table entry:

1. Select the entry.
2. Click Delete. The entry is deleted, and the device is updated.

Defining Multicast Forwarding

The *Multicast Forwarding Page* displays the ports and LAGs attached to the Multicast service group in the Ports and LAGs tables. Ports can be added either to existing groups or to new Multicast service groups. The *Multicast Forwarding Page* permits new Multicast service groups to be created. The *Multicast Forwarding Page* also assigns ports to a specific Multicast service address group.

1. Click **L2 Features > Forward & Filtering > Multicast Forwarding.** The *Multicast Forwarding Page* opens:

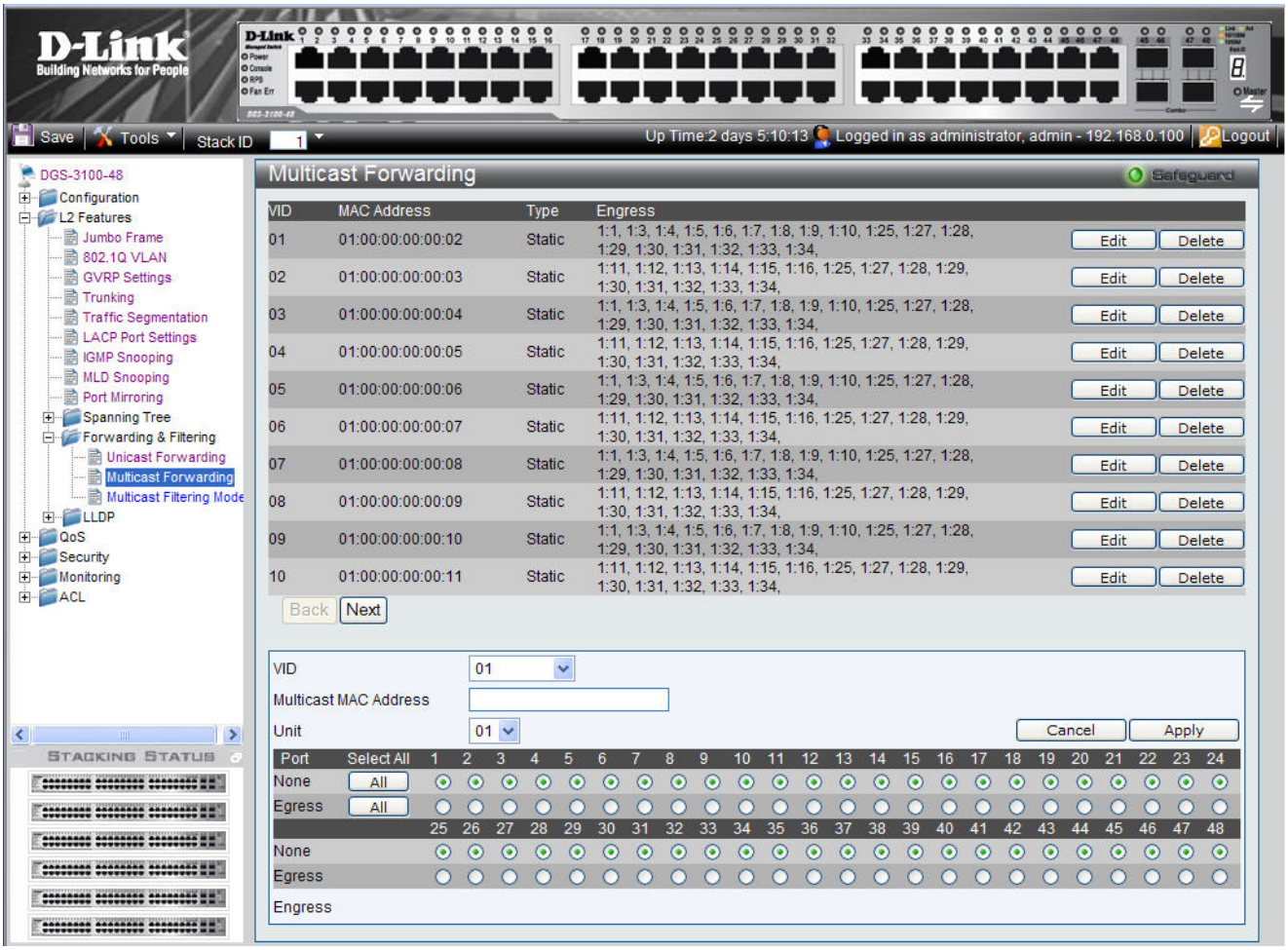


Figure 0–25 Multicast Forwarding Page

The Multicast Forwarding Page contains the following fields:

Field	Description
VID	Defines the VLAN ID
Multicast MAC Address	Defines the Multicast MAC address to which packets are forwarded.
Unit	Defines the unit number.

Field	Description
Egress	Defines the Egress ports per multicast group.

2. Define the VID, Multicast MAC Address, Unit, and Egress fields.
3. Select either all, or individual ports:
   - Click All to select all ports as *None* or *Egress*;
   - Alternatively, click to select the ports individually. The default is 1-48 *None.*
4. Click Apply.The Multicast forwarding settings are applied to the port, and the device is updated.

To restore the default settings:

1. Click Cancel The default settings are restored.
2. To edit a VID entry:
3. Select the entry.
4. Click Edit.
5. Define the fields.
6. Click Apply. The entry is deleted, and the device is updated.

To delete a VID entry:

1. Select the entry.
2. Click Delete VID.

Defining Multicast Filtering

The *Multicast Filtering Mode Page* displays the port filtering mode for unregistered Multicast groups. Ports can filter or forward unregistered Multicast groups. The *Multicast Filtering Mode Page* permits specifying the Multicast filtering mode per port or globally for all ports.

1. Click **L2 Features > Forward & Filtering > Multicast Filtering Mode**. The *Multicast Filtering Mode Page* opens:

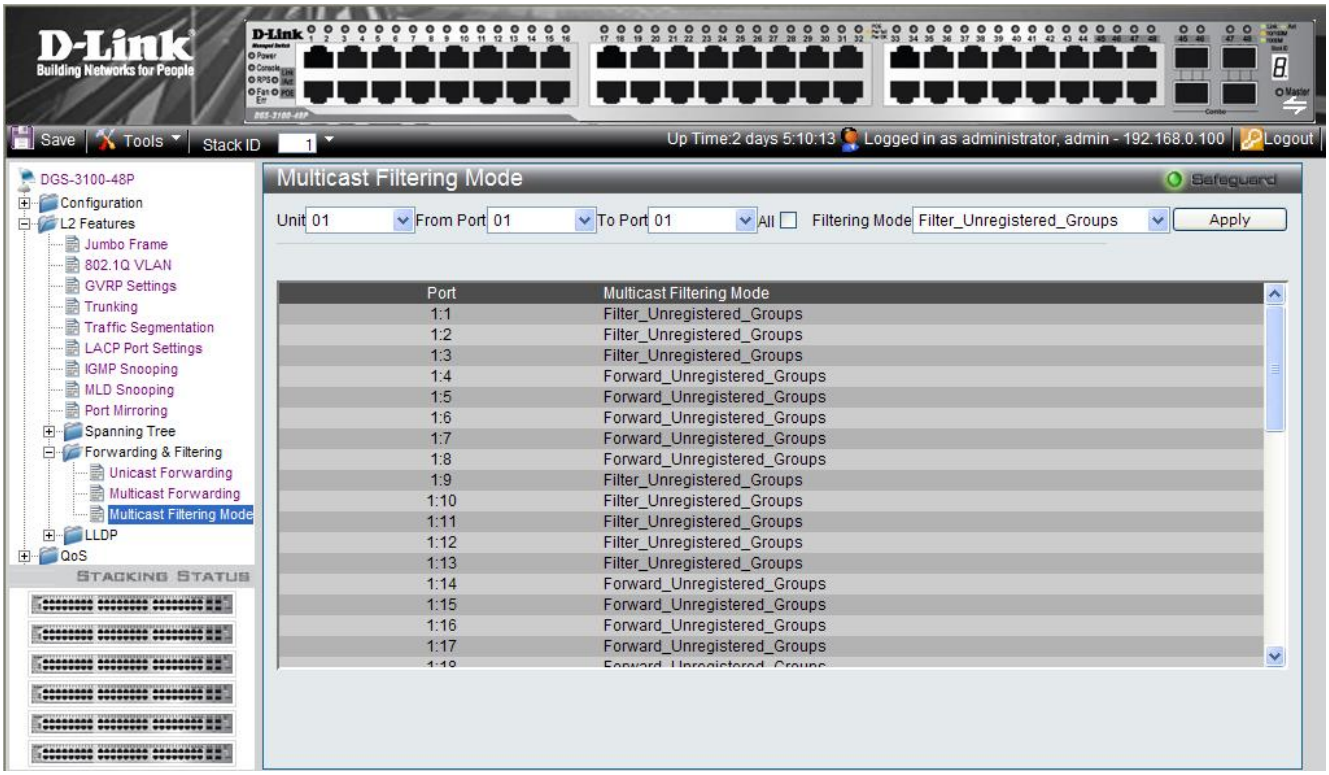


Figure 0–26 Multicast Filtering Mode Page

The Multicast Filtering Mode Page contains the following fields:

Field	Description
Unit	Defines the stacking unit number to specify a port range, or LAG to specify a LAG range.
From Port or **From LAG**	Defines the first port or LAG in a consecutive sequence of ports or LAGs.
To Port or **To LAG**	Defines the last port or LAG in a consecutive sequence of ports or LAGs.
All	Specifies that the filtering mode applies to all ports or LAGs.
Filtering Mode	Defines the multicast filtering mode for unregistered Multicast groups. The possible field values are: *Filter Unregistered Groups* — Filters unregistered Multicast groups. *Forward Unregistered Groups* — Forwards unregistered Multicast groups. This is the default mode.

2. Define the *Unit* and *Filtering Mode* fields.
3. Select either *All* or specify a port (LAG) range in the *From Port* (*From LAG*) and *To Port* (*To LAG*) fields.
4. Click Apply. The Multicast filtering settings are applied to the ports (LAGs), and the device is updated.

Defining DLF Filtering

The *Destination Lookup Failure* (DLF) filtering mode allows the user to define egress filtering for unknown unicast packets. Once an egress port is set to filter/forward DLF packets, DLF traffic on all the VLANs will be configured to filter/forward DLF packets.

The *DLF Filtering Mode Page* allows users to specify DLF filtering per port or globally and define the required filtering mode. By default, the DLF filtering mode is defined as forwarding which causes packet flooding as opposed to packet filtering which minimizes traffic within the network.

1. Click **L2 Features > Forward & Filtering >DLF Filtering Mode.** The *DLF Filtering Mode Page* opens:

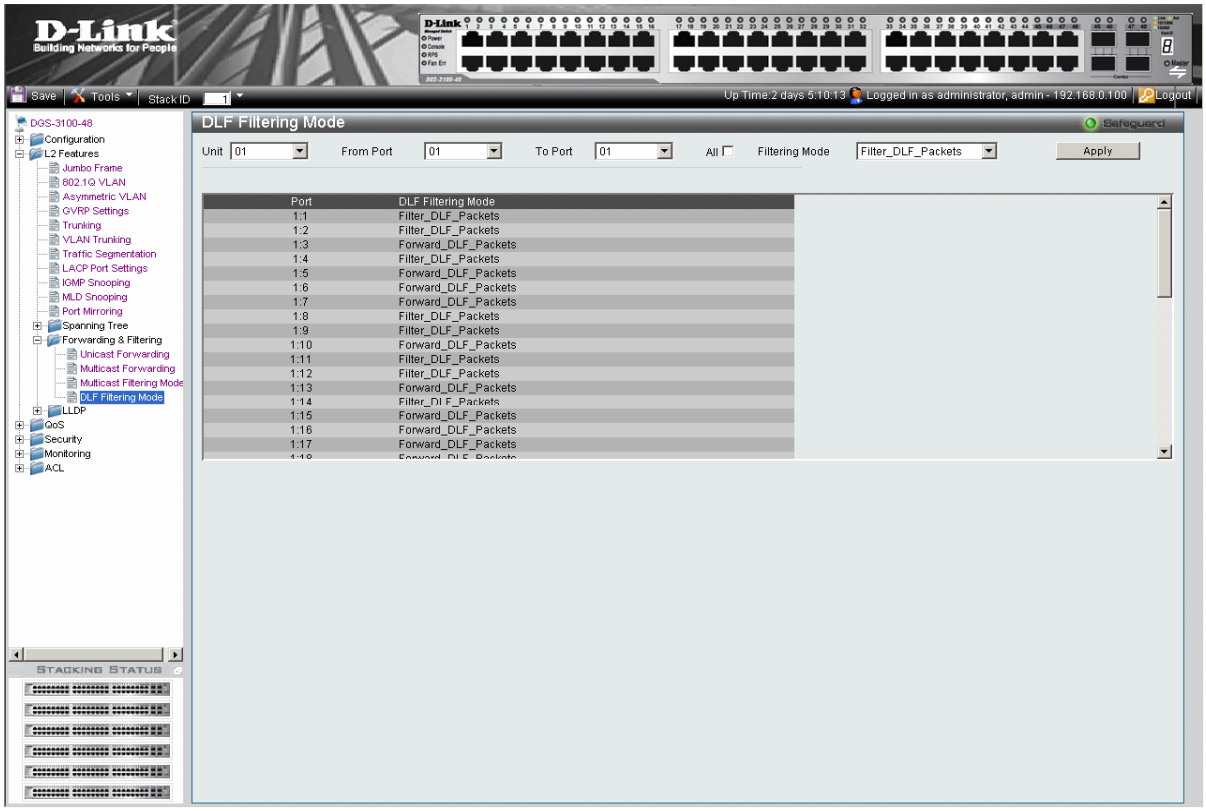


Figure 0–27 DLF Filtering Mode Page

The DLF Filtering Mode Page contains the following fields:

Field	Description
Unit	Defines the stacking unit number to specify a port range, or LAG to specify a LAG range.
From Port or **From LAG**	Defines the first port or LAG in a consecutive sequence of ports or LAGs.
To Port or **To LAG**	Defines the last port or LAG in a consecutive sequence of ports or LAGs.
All	Specifies that the filtering mode applies to all ports or LAGs.
Filtering Mode	Defines the DLF filtering mode for unregistered Multicast groups. The possible field values are: *Filter DLF Packets* — Prevents DLF Packets flooding.. *Forward DLF Packets* — Floods DLF packets within the network. This is the default mode.

2. Define the Unit and Filtering Mode fields.
3. Select either All or specify a port (LAG) range in the From Port (From LAG) and To Port (To LAG) fields.
4. Click Apply .The DLF filtering settings are applied to the ports (LAGs), and the device is updated.

Configuring LLDP

The *Link Layer Discovery Protocol* (LLDP) allows troubleshooting and enhancing network management by discovering and maintaining network topologies over multi-vendor environments. LLDP discovers network neighbors by standardizing methods for network devices to advertise themselves to other systems, and to store discovered information. Device discovery information includes:

Device Identification

Device Capabilities

Device Configuration

The advertising device transmits multiple advertisement message sets in a single LAN packet. The multiple advertisement sets are sent in the packet Type Length Value (TLV) field. LLDP devices must support chassis and port ID advertisement, as well as system name, system ID, system, description, and system capability advertisements.

This section contains information for configuring LLDP parameters, and includes the following topics:

- Defining LLDP Global Settings
- Defining LLDP Port Settings
- Defining LLDP Basic TLV Settings
- Defining LLDP Dot3 TLV Settings
- Viewing LLDP Local Port Information
- Viewing LLDP Remote Port Information

Defining LLDP Global Settings

The *LLDP Global Setting Page* displays LLDP system information and contains parameters for configuring LLDP global settings.

1. Click **L2 Features > LLDP > LLDP Global Setting**. The *LLDP Global Setting Page* opens:

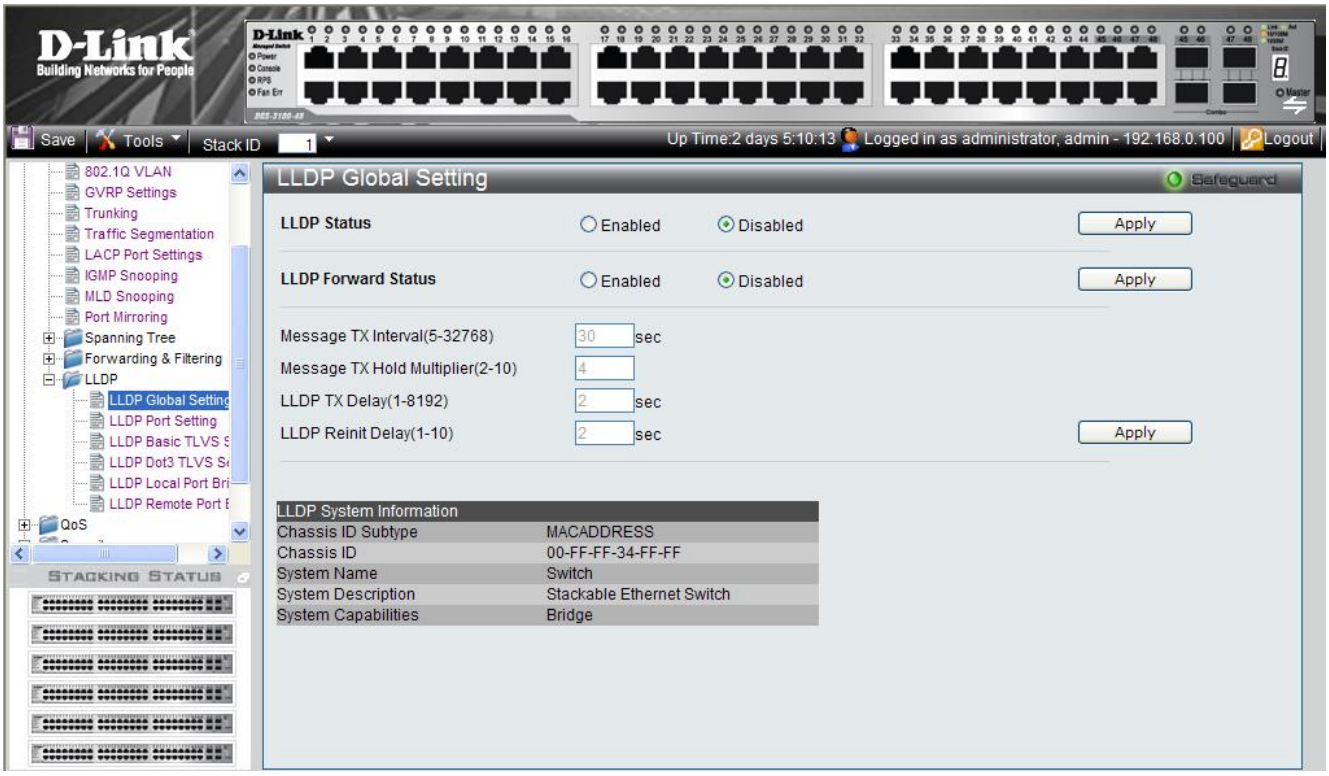


Figure 0–28 LLDP Global Setting Page

The LLDP Global Setting Page contains the following fields:

Field	Description
LLDP Status	Specifies the LLDP status on the device. The possible field values are: *Enabled* — Enables LLDP on the device. *Disabled* — Disables LLDP on the device. This is the default.
LLDP Forward Status	Specifies the LLDP packet forwarding status when LLDP is disabled on the device. The possible field values are: *Enabled* — Enables LLDP packet forwarding on the device. *Disabled* — Disables LLDP packet forwarding on the device.
Message TX Interval	Defines the LLDP message update transmission interval in seconds. The possible field values are 5 – 32768 seconds. The default is 30 seconds.
Message TX Hold Multiplier	Configures the Time-To-Live (TTL) of an LLDP packet, which is the time interval that a receiving device holds an LLDP packet before discarding it. The TTL is defined as the *Message TX Hold Multiplier* times the *Message TX Interval*. The possible field values are 2 – 10. The default is 4.
LLDP TX Delay	Defines the time delay in seconds between successive LLDP frame transmissions initiated by value or status changes. The possible field values are 1 – 8192 seconds. The default is 2 seconds.
LLDP Reinit Delay	Defines the time interval in seconds before reinitializing an LLDP transmission after LLDP is disabled. The possible field values are 1 – 10 seconds. The default is 2 seconds.

2. To configure LLDP Global parameters, select *Enabled* in the *LLDP Status* field and click Apply. LLDP is enabled, and the device is updated.
3. To configure the LLDP packet forwarding status when LLDP is disabled, define the *LLDP Forward Status* field and click Apply. The LLDP packet forwarding status is defined, and the device is updated.
4. To configure LLDP Global parameters when LLDP is enabled, define the *Message TX Interval*, *Message TX Hold Multiplier*, *LLDP TX Delay* and *LLDP Reinit Delay* fields and click Apply. The LLDP packet forwarding status is defined, and the device is updated.

Defining LLDP Port Settings

The *LLDP Port Setting Page* displays LLDP port information and contains parameters for configuring LLDP port settings.

1. Click **L2 Features > LLDP > LLDP Port Setting**. The *LLDP Port Setting Page* opens:

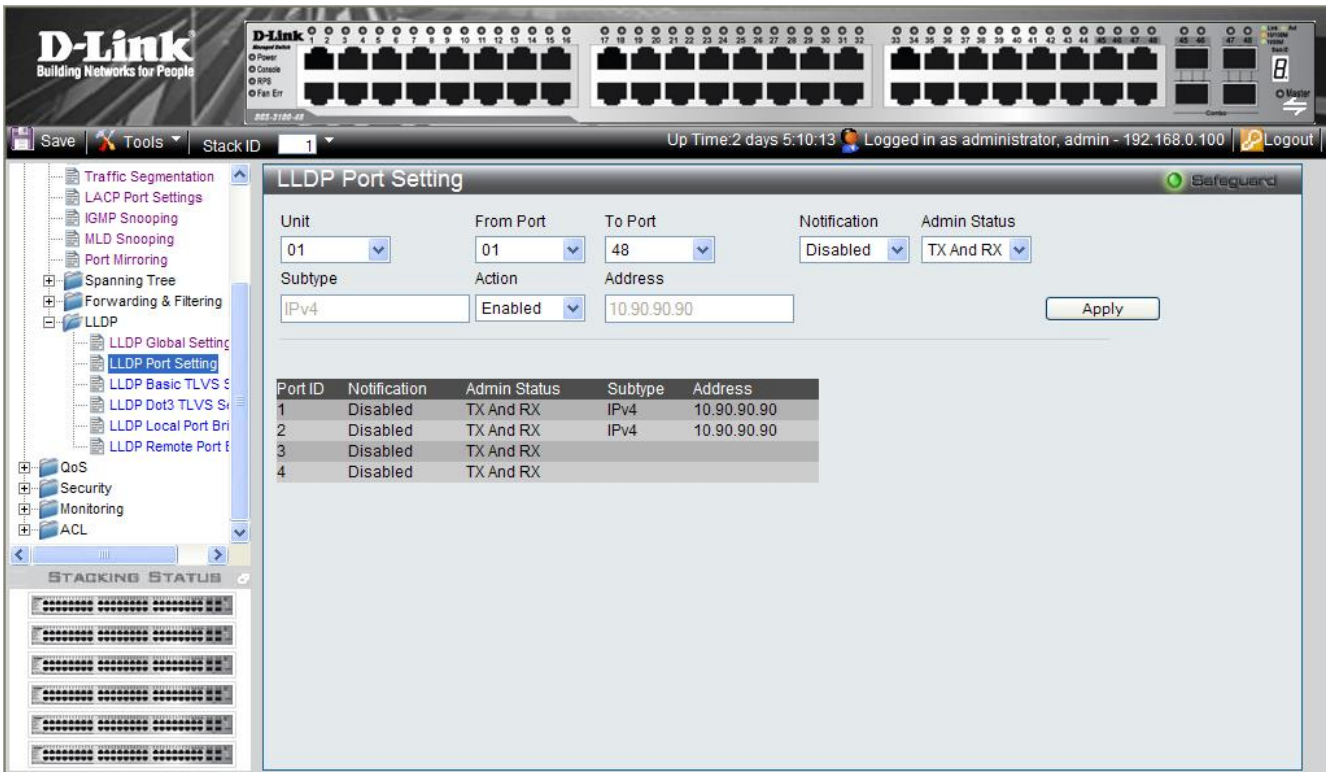


Figure 0–29 LLDP Port Setting Page

The LLDP Port Setting Page contains the following fields:

Field	Description
Unit	Indicates the stacking member for which the LLDP port settings are defined.
From Port	Defines the first port in a consecutive sequence of ports.
To Port	Defines last port in a consecutive sequence of ports.
Notification	Specifies whether notification is sent when an LLDP topology change occurs on the port. The possible field values are: *Enabled* — Enables LLDP notification on the port. *Disabled* — Disables LLDP notification on the port. This is the default.
Admin Status	Specifies the LLDP transmission mode on the port. The possible field values are: *TX* — Enables transmitting LLDP packets only. *RX* — Enables receiving LLDP packets only. *TX and RX* — Enables transmitting and receiving LLDP packets. This is the default. *Disabled* — Disables LLDP on the port.
Subtype	Defines the address subtype. For example, Always IPv4.
Action	Specifies whether the management address is advertised from the port. The possible field values are: *Enabled* — Enables advertisement from the port. This is the default. *Disabled* — Disables advertisement from the port.
Address	Defines the management address advertised from the interface. It is always the Switch's management address.

2. Define the Unit, From Port, To Port, Notification, Admin Status, Subtype, Action and Address fields.
3. Click Apply. The LLDP port settings are defined, and the device is updated.

Defining LLDP Basic TLV Settings

The *LLDP Basic TLVS Setting Page* displays LLDP basic TLV port information and contains parameters for configuring LLDP basic TLV port settings.

1. Click **L2 Features > LLDP > LLDP Basic TLVS Setting**. The *LLDP Basic TLVS Setting Page* opens:

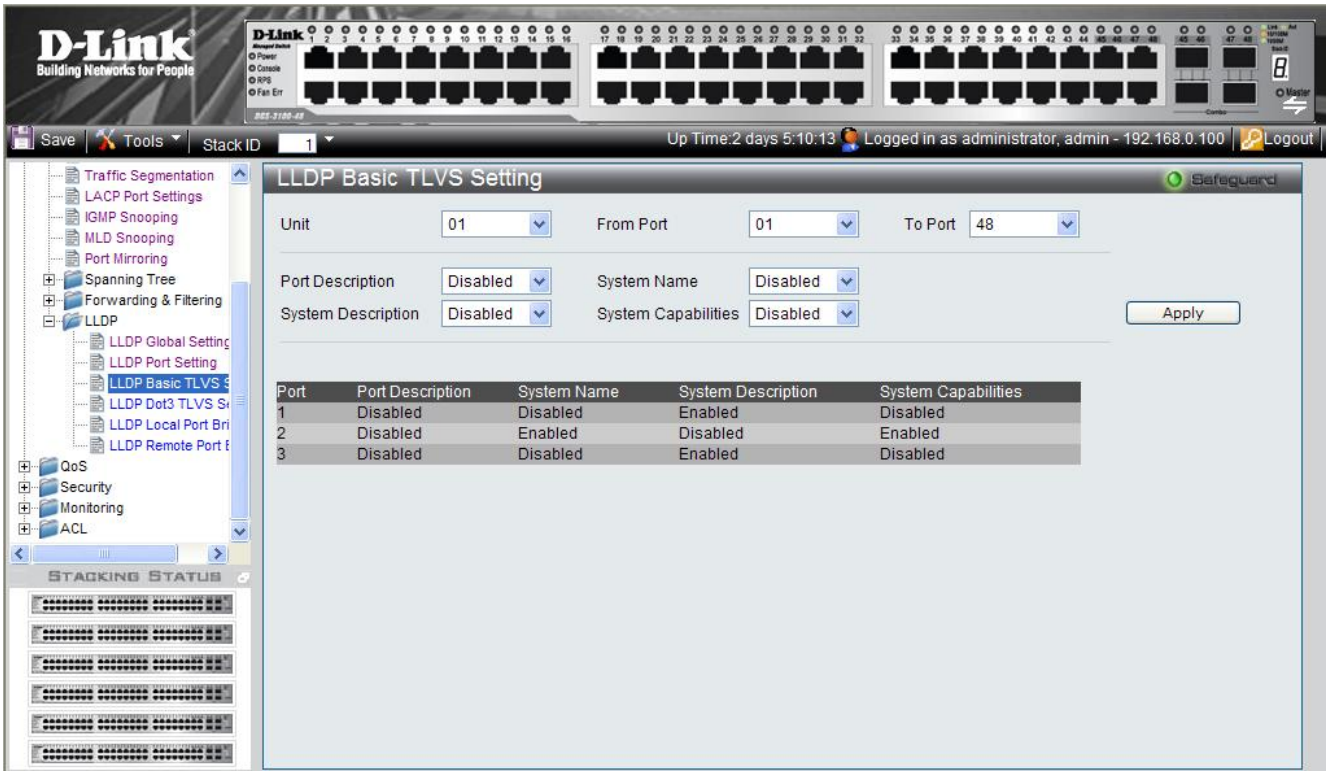


Figure 0–30 LLDP Basic TLVS Setting Page

The LLDP Basic TLVS Setting Page contains the following fields:

Field	Description
Unit	Indicates the stacking member for which the LLDP basic TLV port settings are defined.
From Port	Defines the first port in a consecutive sequence of ports.
To Port	Defines last port in a consecutive sequence of ports.
Port Description	Specifies whether the Port Description TLV is enabled on the port. The possible field values are: *Enabled* — Enables the Port Description TLV on the port. *Disabled* — Disables the Port Description TLV on the port.
System Name	Specifies whether the System Name TLV is enabled on the port. The possible field values are: *Enabled* — Enables the System Name TLV on the port. *Disabled* — Disables the System Name TLV on the port.
System Description	Specifies whether the System Description TLV is enabled on the port. The possible field values are: *Enabled* — Enables the System Description TLV on the port. *Disabled* — Disables the System Description TLV on the port.
System Capabilities	Specifies whether the System Capabilities TLV is enabled on the port. The possible field values are:

Field	Description
	Enabled — Enables the System Capabilities TLV on the port. *Disabled* — Disables the System Capabilities TLV on the port.

2. Define the Unit, From Port, To Port, Port Description, System Name, System Description and System Capabilities fields.
3. Click Apply. The LLDP basic TLV settings are defined, and the device is updated.

Defining LLDP Dot3 TLV Settings

The *LLDP Dot3 TLVS Setting Page* displays LLDP Dot3 TLV port information and contains parameters for configuring LLDP Dot3 TLV port settings.

1. Click **L2 Features > LLDP > LLDP Dot3 TLVS Setting**. The *LLDP Dot3 TLVS Setting Page* opens:

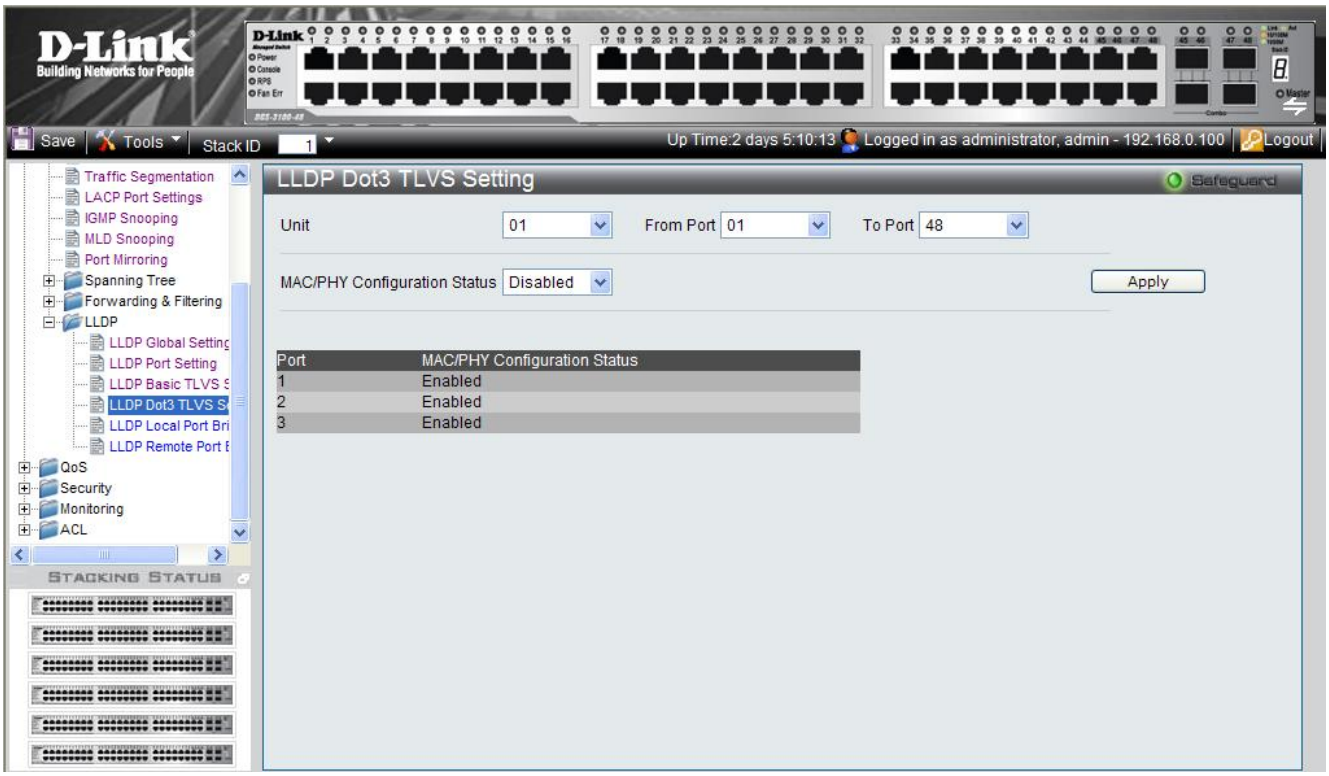


Figure 0–31 LLDP Dot3 TLVS Setting Page

The LLDP Dot3 TLVS Setting Page contains the following fields:

Field	Description
Unit	Indicates the stacking member for which the LLDP dot3 TLV port settings are defined.
From Port	Defines the first port in a consecutive sequence of ports.
To Port	Defines last port in a consecutive sequence of ports.
MAC/PHY Configuration Status	Specifies whether the MAC/PHY Configuration Status is enabled on the port. The possible field values are: *Enabled* — Enables the MAC/PHY Configuration Status on the port. *Disabled* — Disables the MAC/PHY Configuration Status on the port.

2. Define the Unit, From Port, To Port and MAC/PHY Configuration Status fields.
3. Click Apply. The LLDP Dot3 TLV settings are defined, and the device is updated.

Viewing LLDP Local Port Information

The LLDP Local Port Brief Page displays LLDP local port information.

1. Click **L2 Features > LLDP > LLDP Local Port Brief.** The *LLDP Local Port Brief Page* opens:

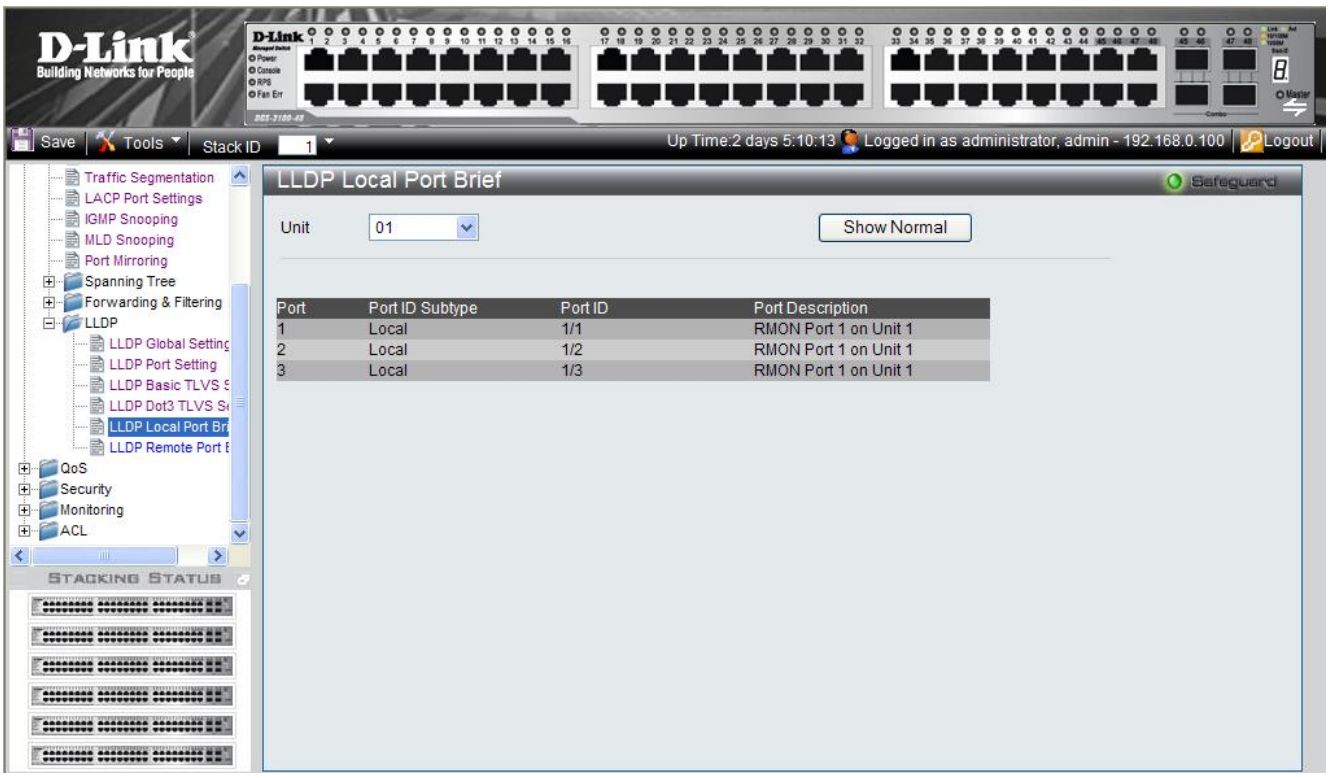


Figure 0–32 LLDP Local Port Brief Page

The LLDP Local Port Brief Page contains the following fields:

Field	Description
Unit	Indicates the stacking member for which the LLDP local port information is displayed.
Port	Indicates the port number.
Port ID Subtype	Displays the port ID subtype.
Port ID	Displays the port ID (Unit number/Port number).
Port Description	Displays the port description.

2. Click Show Normal. The LLDP Local Port Normal Page is displayed.

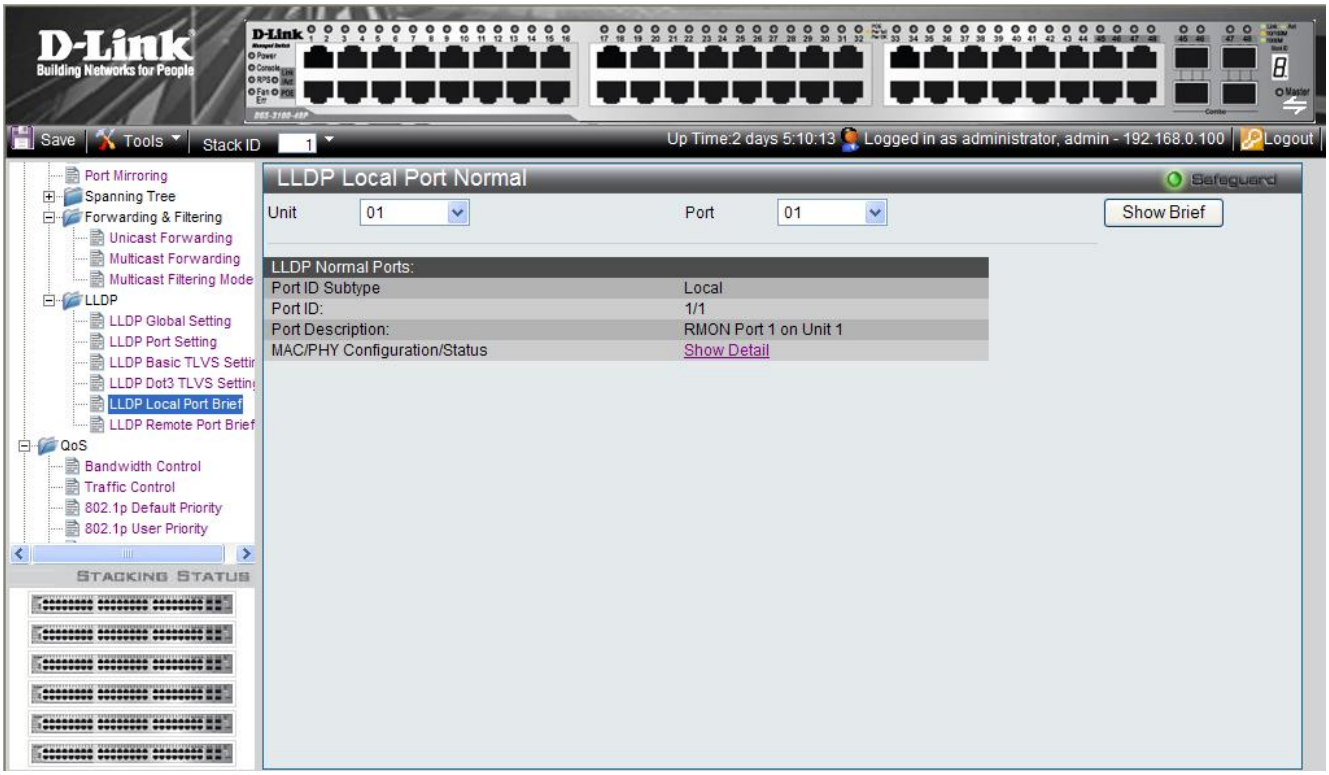


Figure 0–33 LLDP Local Port Normal Page

3. To view the detailed MAC/PHY Configuration Status for the port, click Show Detail. The *LLDP Local Misc Detail Information Page* is displayed**.**

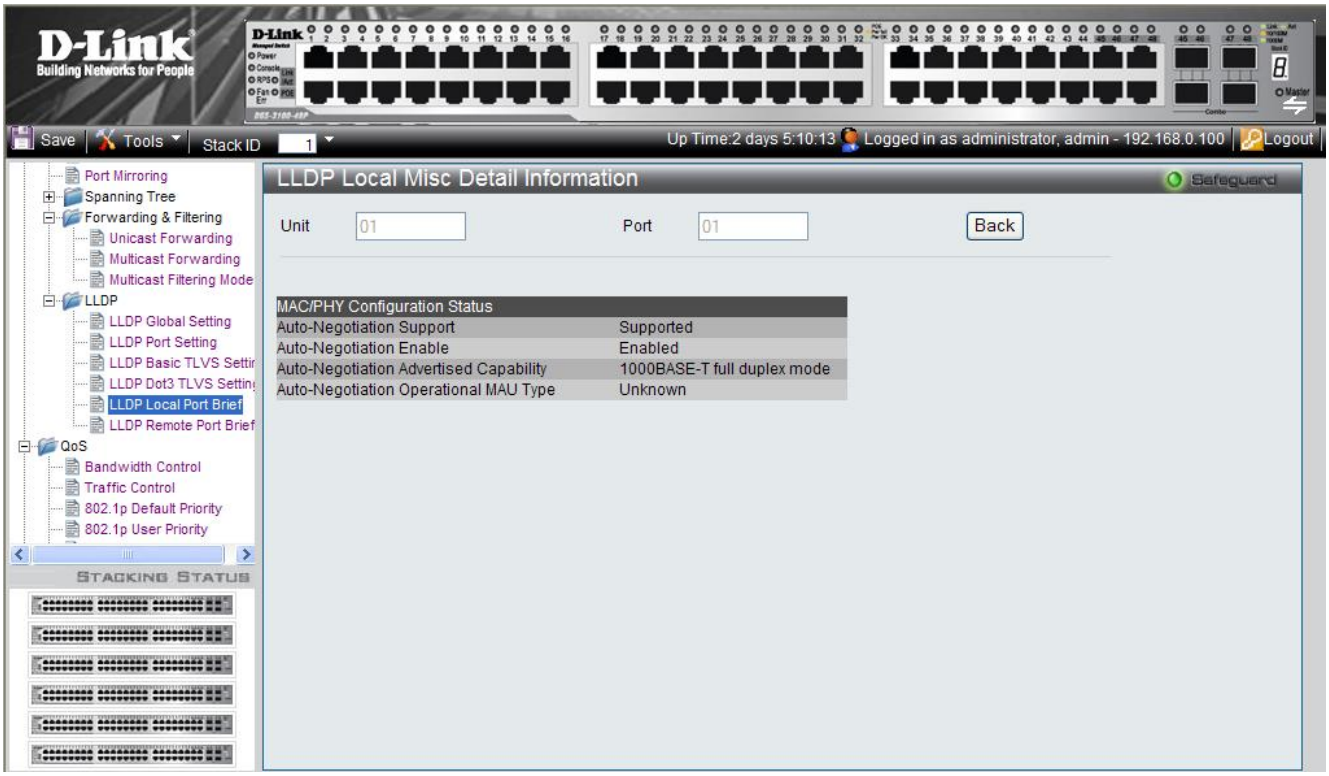


Figure 0–34 LLDP Local Misc Detail Information Page

The LLDP Local Misc Detail Information Page contains the following fields:

Field	Description
Unit	Indicates the stacking member for which the LLDP local detail information is displayed.
Port	Indicates the port number.
Auto-Negotiation Support	Indicates the port speed auto-negotiation support status.
Auto-Negotiation Enable	Indicates the port speed auto-negotiation active status.
Auto-Negotiation Advertised Capability	Displays the port speed auto-negotiation advertised capability. For example, 1000BASE-T full duplex mode.
Auto-Negotiation Operational MAU Type	Displays the Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network. For example, 100BASE-TX full duplex mode.

Viewing LLDP Remote Port Information

The LLDP Remote Port Brief Page displays LLDP remote (neighbor) port information.

1. Click **L2 Features > LLDP > LLDP Remote Port Brief**. The *LLDP Remote Port Brief Page* opens:

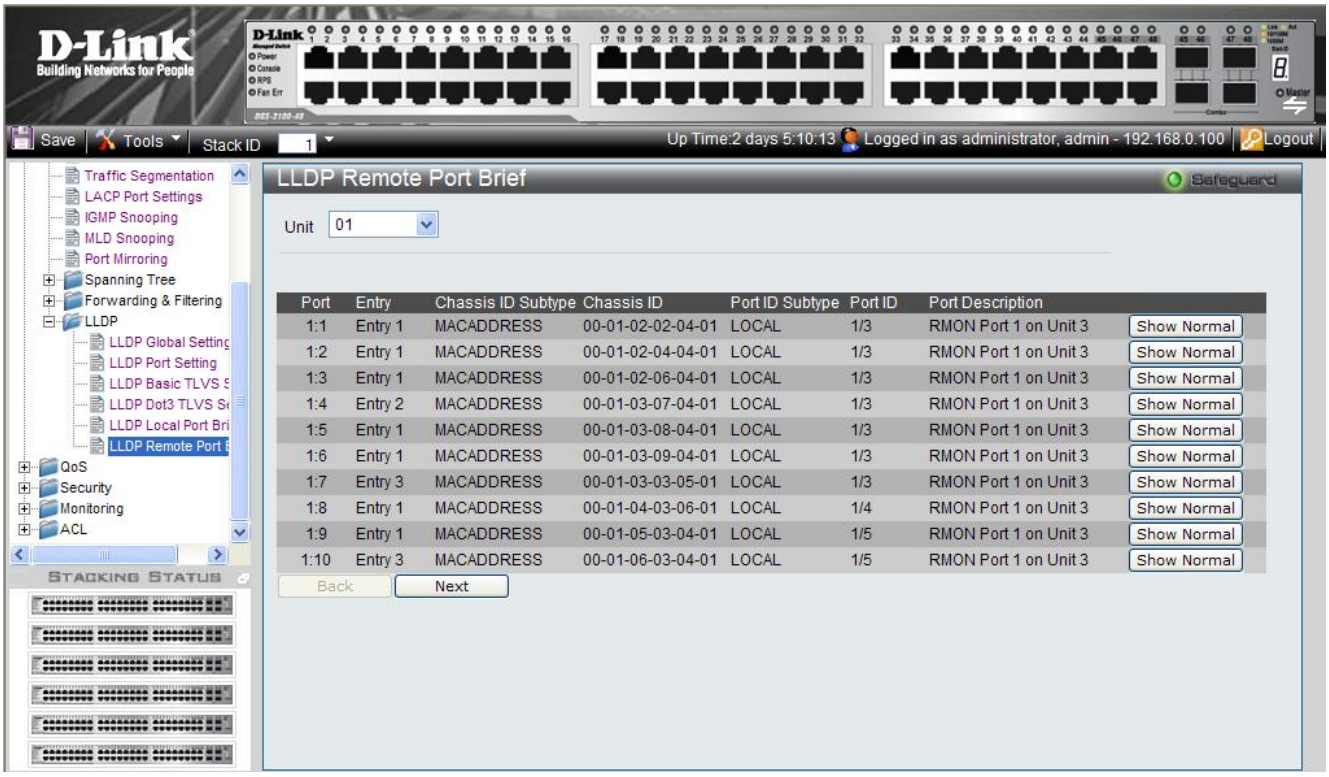

D-Link
Building Networks for People
Save
Tools
Stack ID
1
Up Time:2 days 5:10:13
Logged in as administrator, admin - 192.168.0.100
Logout
Traffic Segmentation
LACP Port Settings
IGMP Snooping
MLD Snooping
Port Mirroring
Spanning Tree
Forwarding & Filtering
LLDP
LLDP Global Setting
LLDP Port Setting
LLDP Basic TLVS
LLDP Dot3 TLVS
LLDP Local Port Bri
LLDP Remote Port
QoS
Security
Monitoring
ACL
STACKING STATUS
LLDP Remote Port Brief
Safeguard
Unit 01
Port Entry Chassis ID Subtype Chassis ID Port ID Subtype Port ID Port Description
1:1 Entry 1 MACADDRESS 00-01-02-02-04-01 LOCAL 1/3 RMON Port 1 on Unit 3 Show Normal
1:2 Entry 1 MACADDRESS 00-01-02-04-04-01 LOCAL 1/3 RMON Port 1 on Unit 3 Show Normal
1:3 Entry 1 MACADDRESS 00-01-02-06-04-01 LOCAL 1/3 RMON Port 1 on Unit 3 Show Normal
1:4 Entry 2 MACADDRESS 00-01-03-07-04-01 LOCAL 1/3 RMON Port 1 on Unit 3 Show Normal
1:5 Entry 1 MACADDRESS 00-01-03-08-04-01 LOCAL 1/3 RMON Port 1 on Unit 3 Show Normal
1:6 Entry 1 MACADDRESS 00-01-03-09-04-01 LOCAL 1/3 RMON Port 1 on Unit 3 Show Normal
1:7 Entry 3 MACADDRESS 00-01-03-03-05-01 LOCAL 1/3 RMON Port 1 on Unit 3 Show Normal
1:8 Entry 1 MACADDRESS 00-01-04-03-06-01 LOCAL 1/4 RMON Port 1 on Unit 3 Show Normal
1:9 Entry 1 MACADDRESS 00-01-05-03-04-01 LOCAL 1/5 RMON Port 1 on Unit 3 Show Normal
1:10 Entry 3 MACADDRESS 00-01-06-03-04-01 LOCAL 1/5 RMON Port 1 on Unit 3 Show Normal
Back
Next

Figure 0–35 LLDP Remote Port Brief Page

The LLDP Remote Port Brief Page contains the following fields:

Field	Description
Unit	Indicates the stacking member for which the LLDP remote port information is displayed.
Port	Indicates the port number.
Entry	Indicates the the device's Media Service Access Point (MSAP) entry number.
Chassis ID Subtype	Displays the chassis ID subtype. For example, MAC address

Field	Description
Chassis ID	Displays the chassis identification of the device transmitting the LLDP frame.
Port ID Subfype	Displays the port ID subtype. For example, IPv4 address.
Port ID	Displays the port ID (Unit number/Port number) of the port transmitting the LLDP frame..
Port Description	Displays the port description.

2. Click Show Normal. The *LLDP Remote Port Normal Page* is displayed.

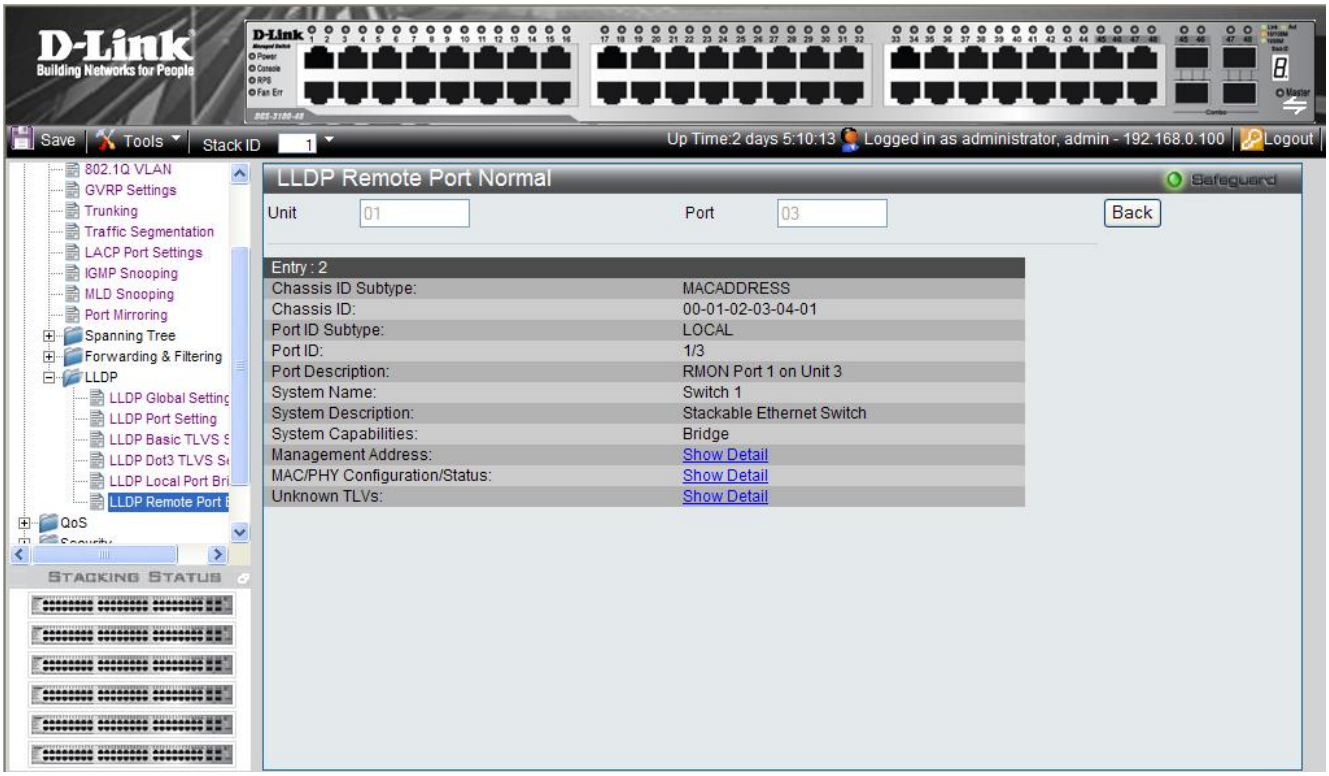


Figure 0–36 LLDP Remote Port Normal Page

3. To view the detailed Management Address information for the entry, click Show Detail. The *LLDP Management Address Detail Information Page* is displayed.

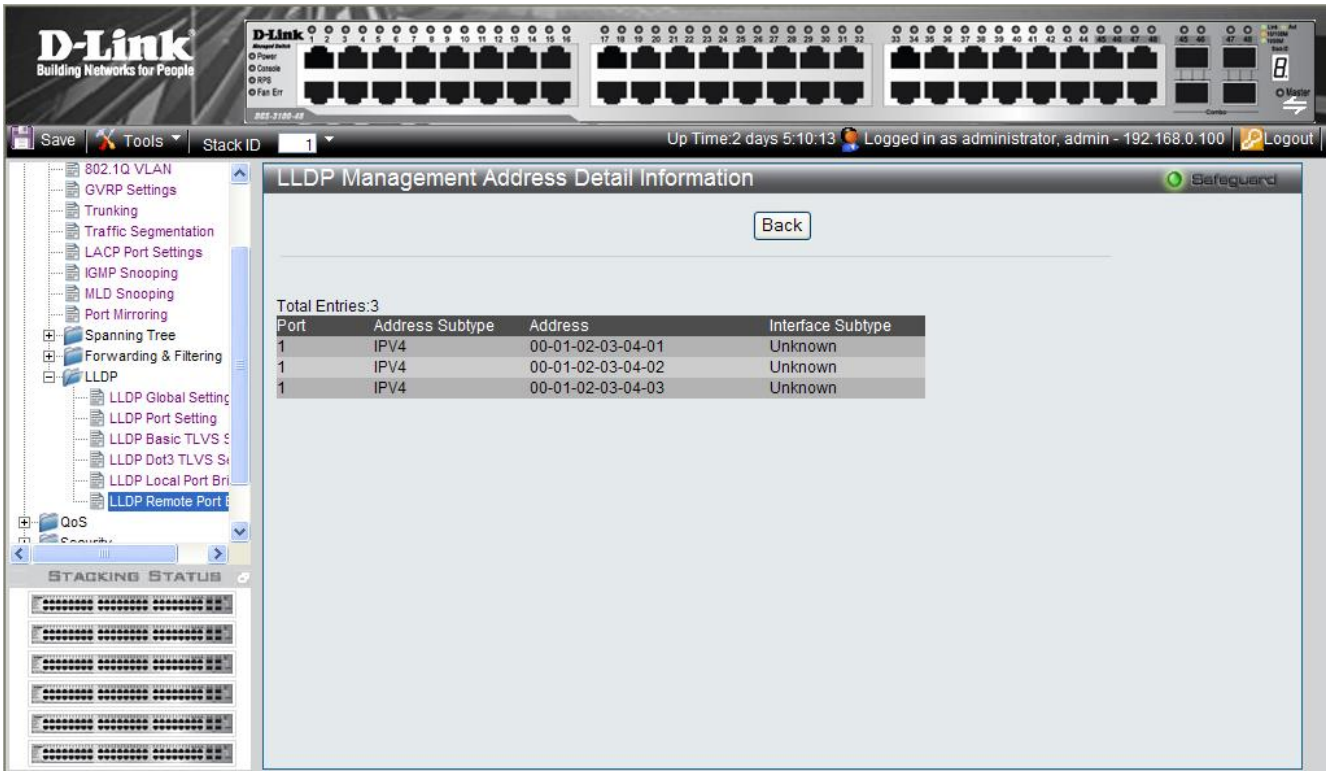


Figure 0–37 LLDP Management Address Detail Information Page

The LLDP Management Address Detail Information Page contains the following fields:

Field	Description
Port	Indicates the port number.
Address Subtype	Displays the managed address subtype. For example, MAC or IPv4
Address	Displays the managed address.
Interface Subtype	Displays the port subtype.

4. Click Back to return to the LLDP Remote Port Normal Page.
5. To view the detailed MAC/PHY Configuration/Status information for the entry, click Show Detail. The *LLDP Remote Misc Detail Information Page* is displayed.

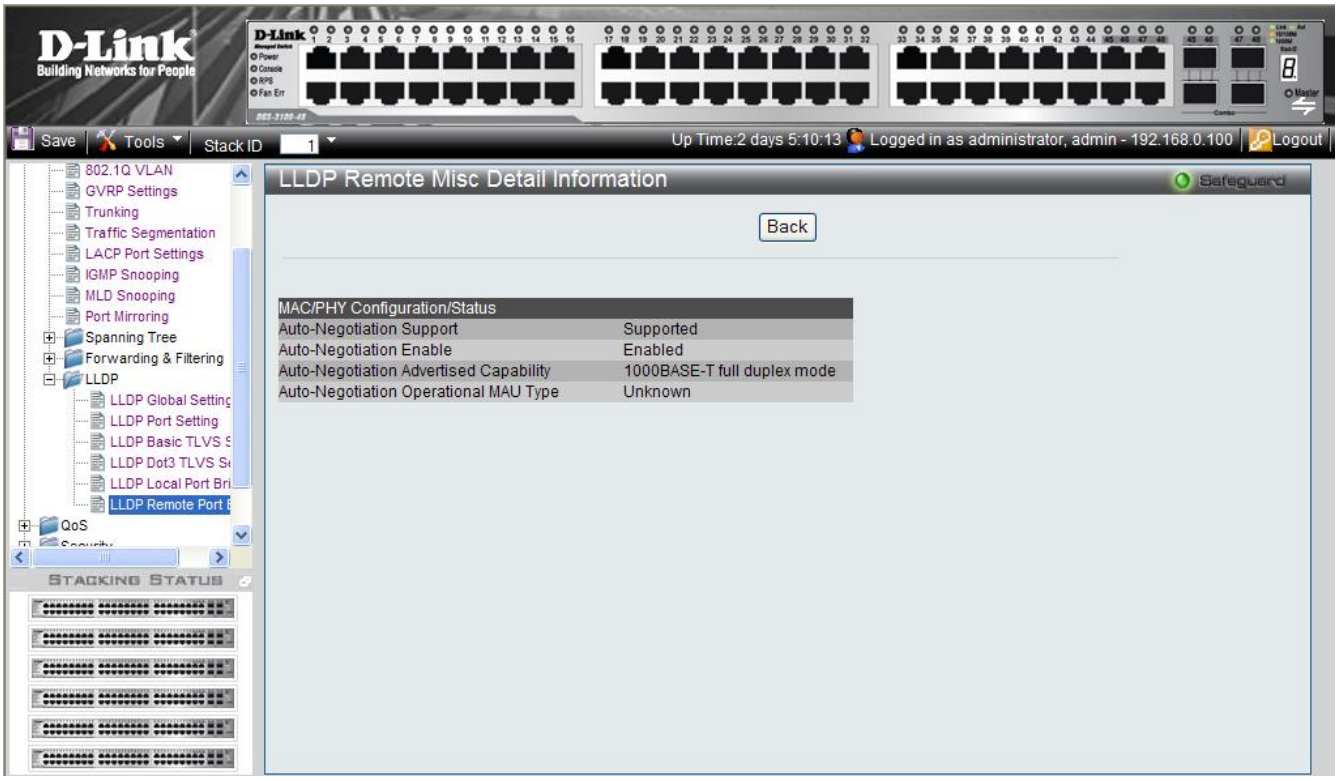


Figure 0–38 LLDP Remote Misc Detail Information Page

6. Click Back to return the LLDP Remote Port Normal Page.
7. To view the detailed information for unknown TLVs for the entry, click Show Detail. The *LLDP Remote Unknown TLVs Detailed Information Page* is displayed.

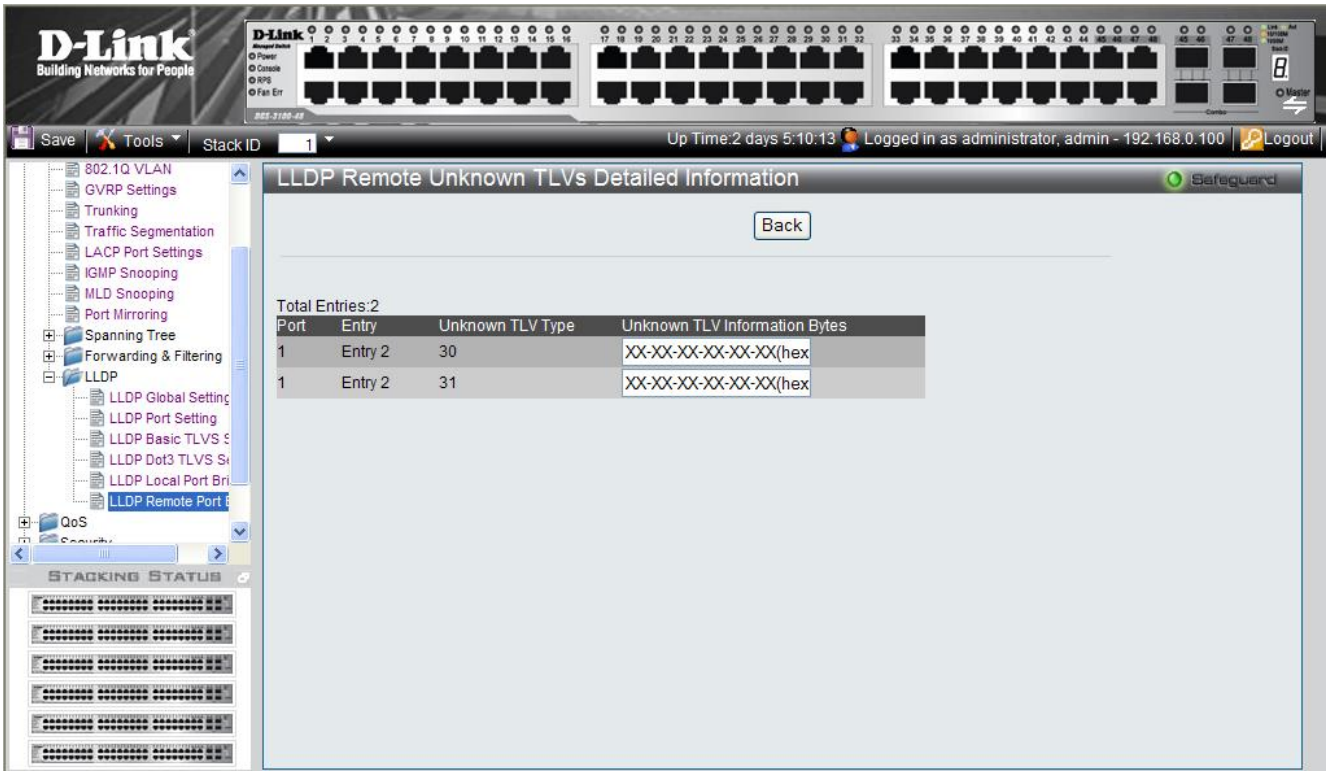


Figure 0–39 LLDP Remote Unknown TLVs Detailed Information Page

The LLDP Remote Unknown TLVs Detailed Information Page contains the following fields:

Field	Description
Port	Indicates the port number.
Entry	Indicates the entry number.
Unknown TLV Type	Indicates the unknown TLV type field
Unknown TLV Information Bytes	Displays the unknown TLV information bytes in hexadecimal format.

Configuring Voice VLAN

Voice VLAN enables network administrators to improve VoIP service by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. VoIP traffic has a preconfigured OUI prefix in the source MAC address. Network administrators can configure VLANs on which voice IP traffic is forwarded. Non-VoIP traffic is dropped from the Voice VLAN in Auto Voice VLAN Secure mode. Voice VLAN also provides QoS, ensuring that the quality of voice does not deteriorate if the IP traffic is received unevenly. The system supports one Voice VLAN.

There are two operational modes for IP Phones:

- IP phones are configured with VLAN-mode as enabled, ensuring that tagged packets are used for all communications.
- If the IP phone's VLAN-mode is disabled, the phone uses untagged packets. The phone uses untagged packets while retrieving the initial IP address through DHCP. The phone eventually uses the Voice VLAN and begins sending tagged packets.

This section contains the following topics:

- Defining Voice VLAN Global Settings
- Defining Voice VLAN Port Settings
- Defining OUIs
- Defining Voice VLAN Global Settings

The *Voice VLAN Global Setting Page* displays the parameters for creating and configuring the Voice VLAN global settings.

1. Click **L2 Features > Voice VLAN > Global Setting**. The *Voice VLAN Global Setting Page* opens:

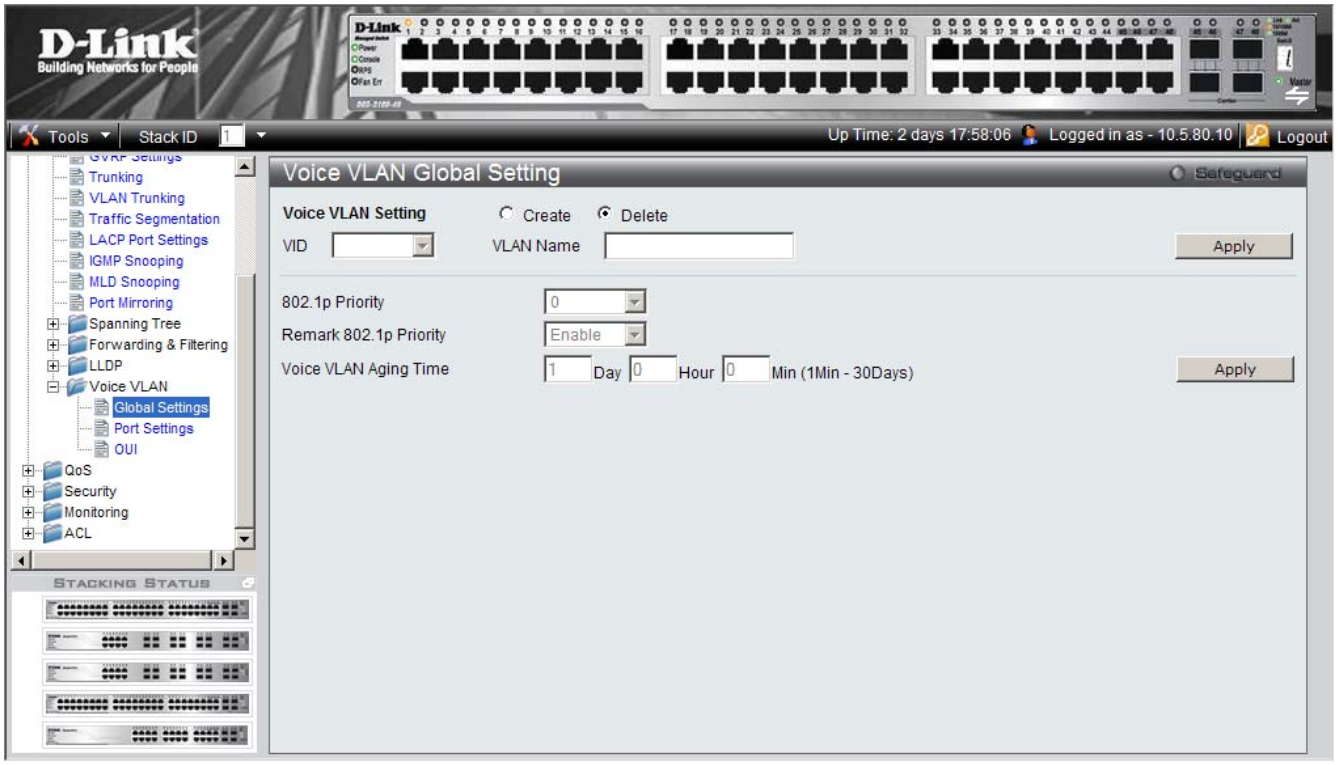


Figure 0–40 Voice VLAN Global Setting Page

The Voice VLAN Global Setting Page contains the following fields:

Field	Description
Voice VLAN Setting	Specifies the action to take. The possible field values are: • Create — Creates the Voice VLAN. • Delete — Removes Voice VLAN from the device. This is the default.
VID	Selects the Voice VLAN ID number.

Field	Description
VLAN Name	Defines the name of the Voice VLAN
802.1p Priority	Prioritization that groups packets into various traffic classes
Remark 802.1p Priority	Specifies whether 802.1p Priority replaces the 802.1p Priority written in the packet (Enable) or used only for forwarding within the device (Disable).
Voice VLAN Aging Time	Indicates the amount of time after the last IP phone's OUI was received on a port, after which this port will be removed from the Voice VLAN. The default time is one day. The field format is Day, Hour, Minute. The aging time starts after the MAC Address is aged out from the Dynamic MAC Address table. The default time is for this is 300 seconds.

2. To configure Voice VLAN Global Settings, select *Create* in the *Voice VLAN Setting* field, select a *VID*, enter a *VLAN Name*.
3. To configure the 802.1p Priority, select the priority in the *802.1p Priority* field and enable or disable *Remark 802.1p Priority*.
4. To configure Voice VLAN Aging, define the *Voice VLAN Aging Time* field.
5. Click Apply. The Voice VLAN is created, its global settings are defined, and the device is updated.

Defining Voice VLAN Port Settings

The Voice VLAN Port Setting Page contains fields for assigning ports or LAGs to the voice VLAN.

1. Click **L2 Features > Voice VLAN > Port Settings**. The *Voice VLAN Port Setting Page* opens:

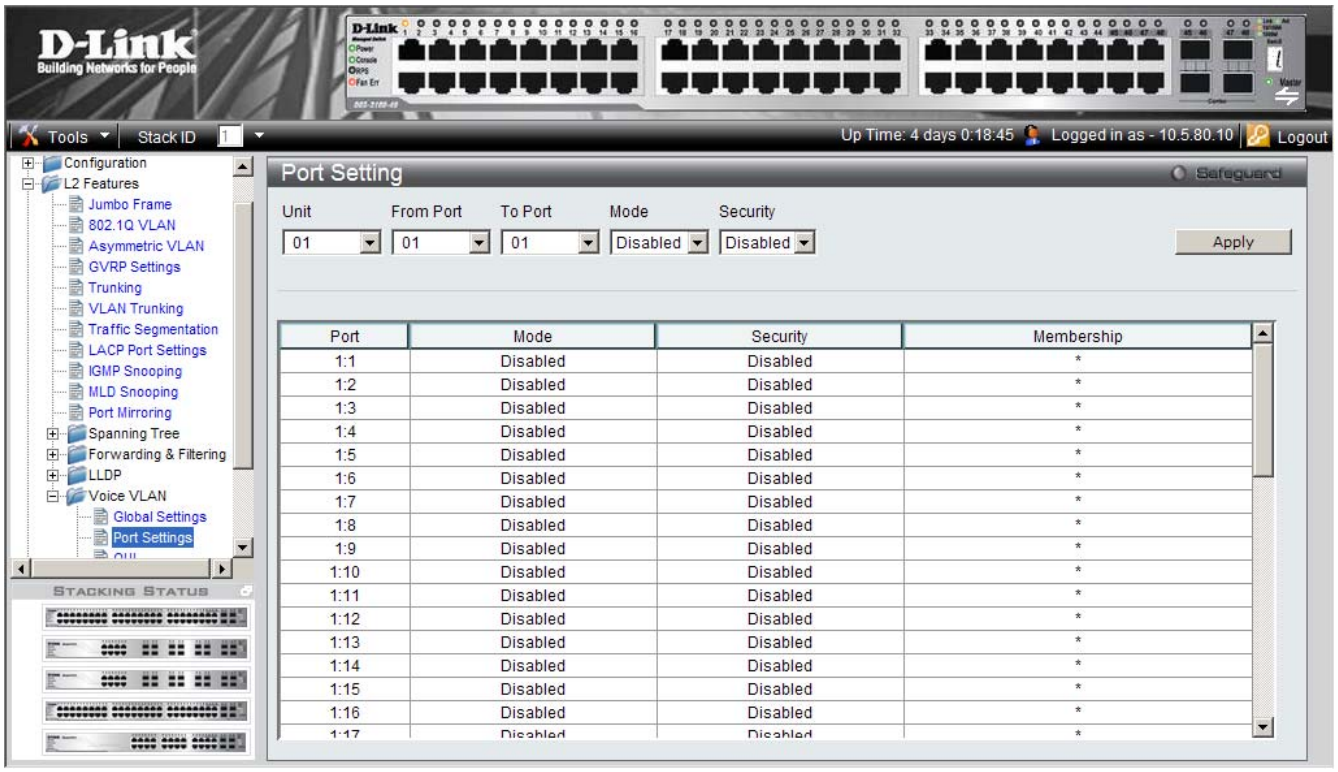


Figure 0–41 Voice VLAN Port Setting Page

The Voice VLAN Port Setting Page contains the following fields:

Field	Description
Unit	Defines the stacking member for which the Voice VLAN parameters are displayed.
From Port	Defines from which port number bandwidth settings are displayed.
To Port	Defines to which port number bandwidth settings are displayed.
Mode	Defines the Voice VLAN mode. The possible field values are: • Disabled — Disables the selected *port* on the Voice VLAN. • Auto — Indicates that if traffic with an IP Phone MAC address is transmitted on the port/LAG, the *port* joins the Voice VLAN. Timeout is as defined in the Defining Voice VLAN Global Settings section. If the MAC Address of the IP phones OUI was added manually to a port in the Voice VLAN, the user cannot add it to the Voice VLAN.
Security	Indicates if port security is enabled on the Voice VLAN. Port security ensures that packets arriving with an unrecognized OUI are dropped. The possible field values are: • Enable — Enables port security on the Voice VLAN. • Disable — Disables port security on the Voice VLAN.
Membership	Indicates whether the Voice VLAN member is a static or dynamic member. Dynamic indicates that the VLAN membership was dynamically created when a packet with Voice VLAN OUI was captured by the device. Static indicates that the VLAN membership is user-defined. An * indicates that the port is not a member of the Voice VLAN. This is only used when Voice VLAN is disabled on this port.

2. To configure Voice VLAN Port Settings, select the particular unit, as well as the range of ports to set. Select a *Mode*, and a *Security* setting, and click Apply. The Voice VLAN Ports are set, and the device is updated.

Defining OUIs

The *OUI Setting Page* lists the Organizationally Unique Identifiers (OUIs) associated with the Voice VLAN. The first three bytes of the MAC Address contain a manufacturer identifier. While the last three bytes contain a unique station ID. Using the OUI, network managers can add specific manufacturer's MAC addresses to the OUI table. Once the OUIs are added, all traffic received on the Voice VLAN ports from the specific IP phone with a listed OUI, is forwarded on the voice VLAN.

1. Click **L2 Features > Voice VLAN > OUI**. The *OUI Setting Page* opens:

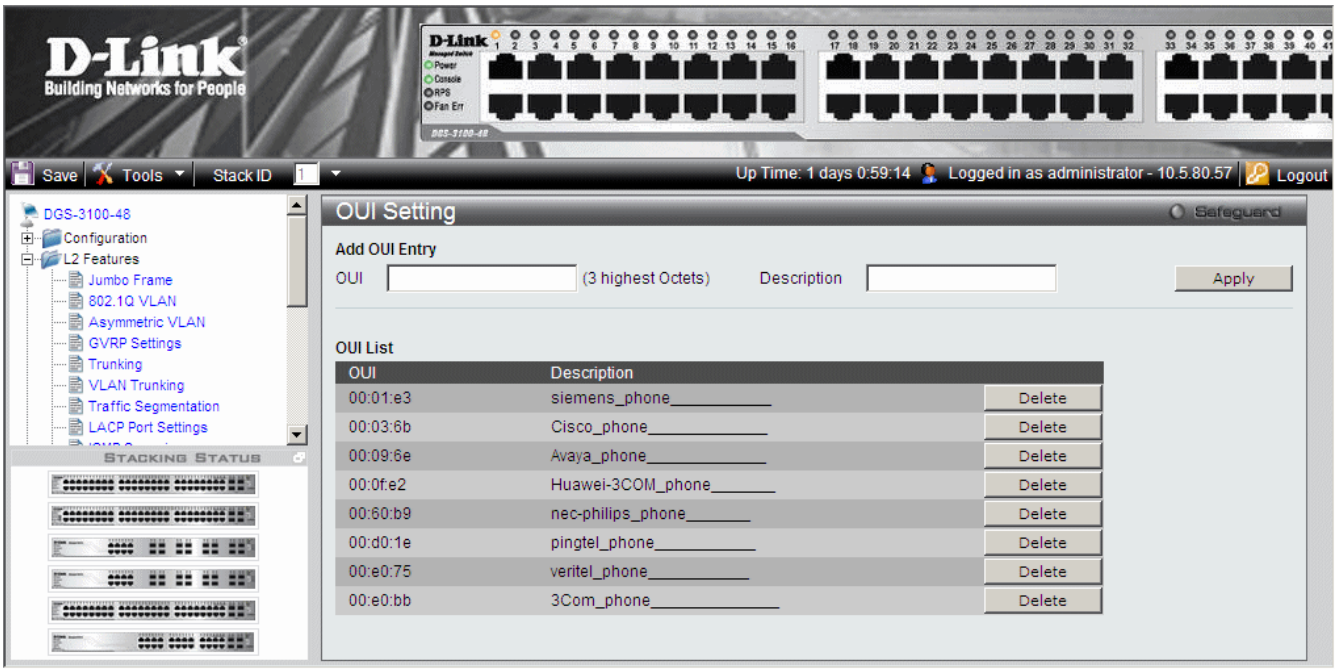


Figure 0–42 OUI Setting Page

The OUI Setting Page contains the following fields:

Field	Description
OUI	Defines the manufacturer's identifier, which is the first three bytes of the MAC address for the devices.
Description	Provides a description of the OUI of up to 32 characters.

2. To configure a new OUI entry, enter the OUI and a description, and click Apply. The OUI will be added to the list, and the device is updated.

The following OUIs are pre-defined:

OUI Entry	Description
00:01:e3	Siemens AG phone
00:03:6b	Cisco phone
00:09:6e	Avaya phone
00:0f:e2	Huawei 3Com phone
00:60:b9	Philips and NEC AG phone
00:d0:1e	Pingtel phone
00:e0:75	Veritel phone
00:e0:bb	3COM phone

4

CONFIGURING QUALITY OF SERVICE

Configuring 1p

Priority tagging is an IEEE 802.1p defined standard function designed to provide a means of managing traffic on networks where many different types of data are transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time-critical data over congested networks. The quality of applications dependent on such data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

IEEE 802.1p standard-compliant network devices recognize the priority level of data packets and can assign priority labels or tags to packets, as well as strip priority tags from packets. The priority tag determines the packet's degree of expeditiousness and the queue to which it is assigned.

Priority tags are assigned values from 0 to 7, with 0 being assigned to the lowest priority data, and 7 to the highest. Generally, tag 7 is used for data associated with video or audio applications, sensitive to even slight delays, or for data from specified end users whose data transmissions warrant special consideration.

The switch enables increased definition for handling priority tagged data packets on the network. Using queues to manage priority tagged data enables user-specification for the data's relative priority to suit the needs of the network. Circumstances can arise where it is advantageous to group two or more different tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 1, be reserved for the data packets with a priority value of 7.

1) Classes not Queues should be used when explaining traffic handling techniques.
2) The ratio is Class0:Class1:Class2:Class3 = 1:2:4:8

A Weighted Round Robin system is employed on the switch to determine the rate which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 1, clears four packets for every packet which cleared from Queue 0.

It is important that the priority queue settings on the switch are for all ports, and all devices connected to the switch are affected. The priority queuing system is especially beneficial for networks that employ priority tag assignment capable switches.

QoS is an implementation of the IEEE 802.1p standard that allows network administrators a method of reserving bandwidth for important functions that require a large bandwidth or have a high priority, such as VoIP (voice-over Internet Protocol), Web browsing applications, file server applications or video conferencing. Not only a larger bandwidth can be created, but also a less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and in turn prioritized. View the following map to see how the DGS-3100 series implements 802.1P priority queuing.

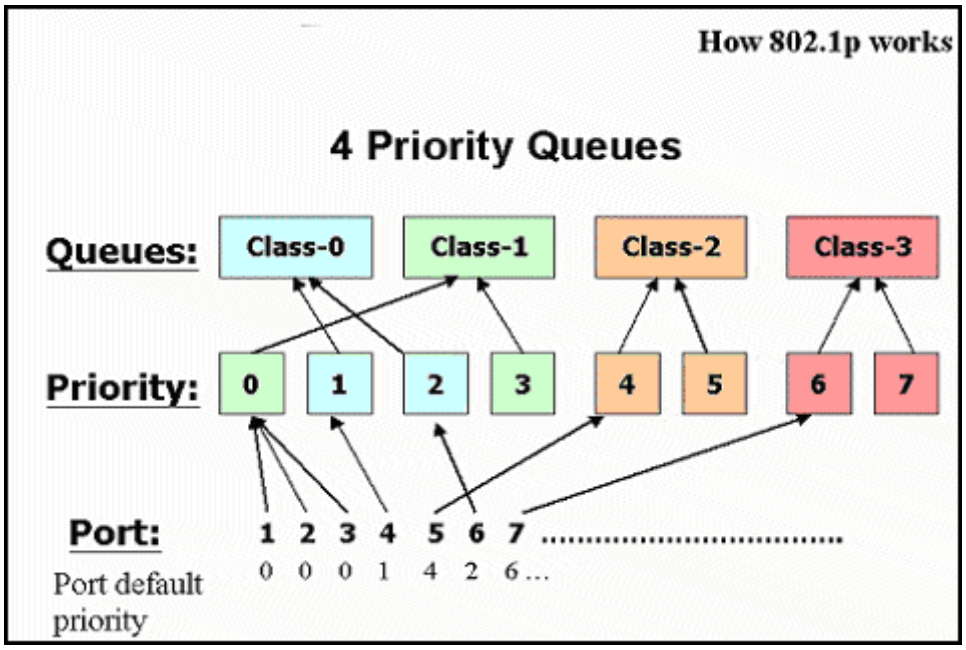


Figure 4-1 Mapping QoS on the Switch

The picture above shows the default priority setting for the Switch. Class-3 has the highest priority of the four priority queues on the Switch. In order to implement QoS, the user is required to instruct the Switch to examine the header of a packet to see if it has the proper identifying tag tagged. Then the user may forward these tagged packets to designated queues on the Switch where they will be emptied, based on priority.

For example, let us say a user wishes to have a video conference between two remotely set computers. The administrator can add priority tags to the video packets being sent out, utilizing the Access Profile commands. Then, on the receiving end, the administrator instructs the Switch to examine packets for this tag, acquires the tagged packets and maps them to a class queue on the Switch. Then in turn, the administrator will set a priority for this queue so that it will be emptied before any other packet is forwarded. This process results in the end user receiving all packets sent as quickly as possible, thus prioritizing the queue and allowing for an uninterrupted stream of packets, which optimizes the use of bandwidth available for the video conference.

Understanding QoS

The Switch has four priority queues. These priority queues are labeled as 3 (the highest queue) to 0 (the lowest queue). The eight (0-7) priority tags, specified in IEEE 802.1p are mapped to the Switch's priority tags as follows:

- Priorities 1 and 2 are assigned to the Switch's Q0 queue.
- Priorities 0 and 3 are assigned to the Switch's Q1 queue.
- Priorities 4 and 5 are assigned to the Switch's Q2 queue.
- Priorities 6 and 7 are assigned to the Switch's Q3 queue.

For strict priority-based scheduling, any packets residing in the higher priority queues are transmitted first. Multiple strict priority queues empty based on their priority tags. Only when these queues are empty, are packets of lower priority transmitted.

For weighted round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight.

For weighted round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

For weighted round-robin queuing, if the weight for a CoS is set to 0, then it will stop processing the packets from this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common weighted round-robin scheme.

Strict Priority should be configured at higher class than WRR.

If the user configures WRR, at least two queues should be configured as WRR.

Remember that the DGS-3100 series has four priority queues (and eight Classes of Service) for each port on the Switch.

This section contains the following topics:

- Defining Bandwidth Settings
- Configuring Storm Control
- Mapping Ports to Packet Priorities
- Mapping Priority to Classes (Queues)
- Configuring QoS Scheduling Mechanism
- Defining DSCP User Priority
- Defining Multi-Layer CoS Settings

Defining Bandwidth Settings

The *Bandwidth Control Page* allows network managers to define the bandwidth settings for a specified interface.

1. Click **QoS > Bandwidth Control**. The *Bandwidth Control Page* opens:

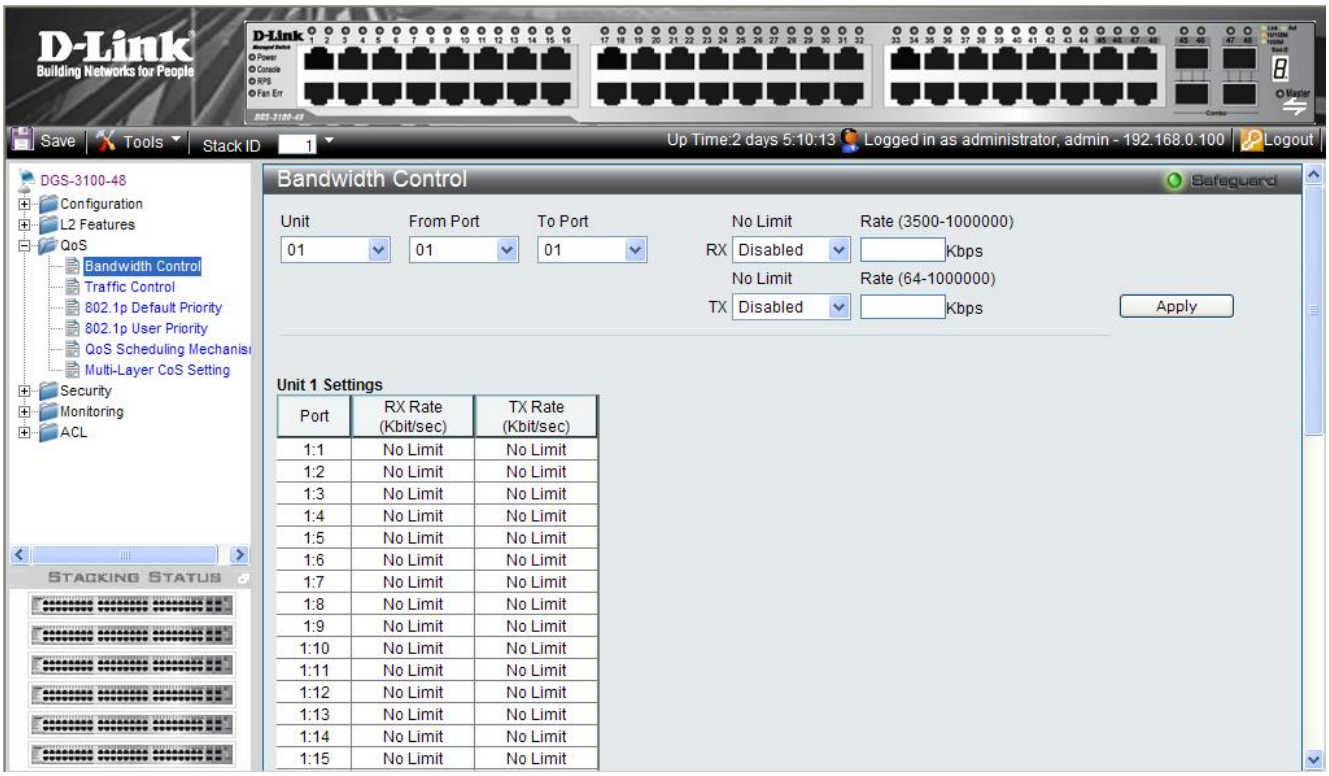


Figure 4-2 Bandwidth Control Page

The Bandwidth Control Page contains the following fields:

Field	Description
Unit	Defines the stacking member for which the bandwidth parameters are displayed
From Port	Defines from which port number bandwidth settings are displayed.
To Port	Defines to which port number bandwidth settings are displayed.
RX No Limit	Defines if ingress bandwidth limitation is assigned to the port. The field value options are: *Enabled* — Ensures no bandwidth limitations on the port. (This is the default value). *Disabled* —Enables ingress bandwidth limitations on the port. When disabled, user can enter a limit value in the RX Rate field.
RX Rate (3500-1000000) kbps	Specifies the maximum ingress rate on the port. The possible field range is 3500 – 1000000 Kbps
TX No Limit	Specifies whether egress bandwidth limitation applies to the port. The possible field values are: *Enabled* — Specifies no egress bandwidth limitations on the port. (This is the default value). *Disabled* —Enables egress bandwidth limitations on the port. When disabled, the user can enter a limit value in the *TX Rate* field.
TX Rate (64-1000000) Kbps	Specifies the maximum egress rate on the port. The possible field range is 64 – 1000000 Kbps.

2. Define the Unit, From Port, To Port, No Limit and Ingress Rate fields.
3. Click Apply. The bandwidth settings are defined, and the device is updated.

Configuring Storm Control

Storm control limits the amount of Multicast, Broadcast and Unknown Unicast frames accepted and forwarded by the device. When Layer 2 frames are forwarded, Broadcast, Multicast and Unknown Unicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes on all ports.

A Broadcast Storm is a result of an excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, straining network resources or causing the network to time out.

1. Click **Qos > Traffic Control**. The *Traffic Control Settings Page* opens:

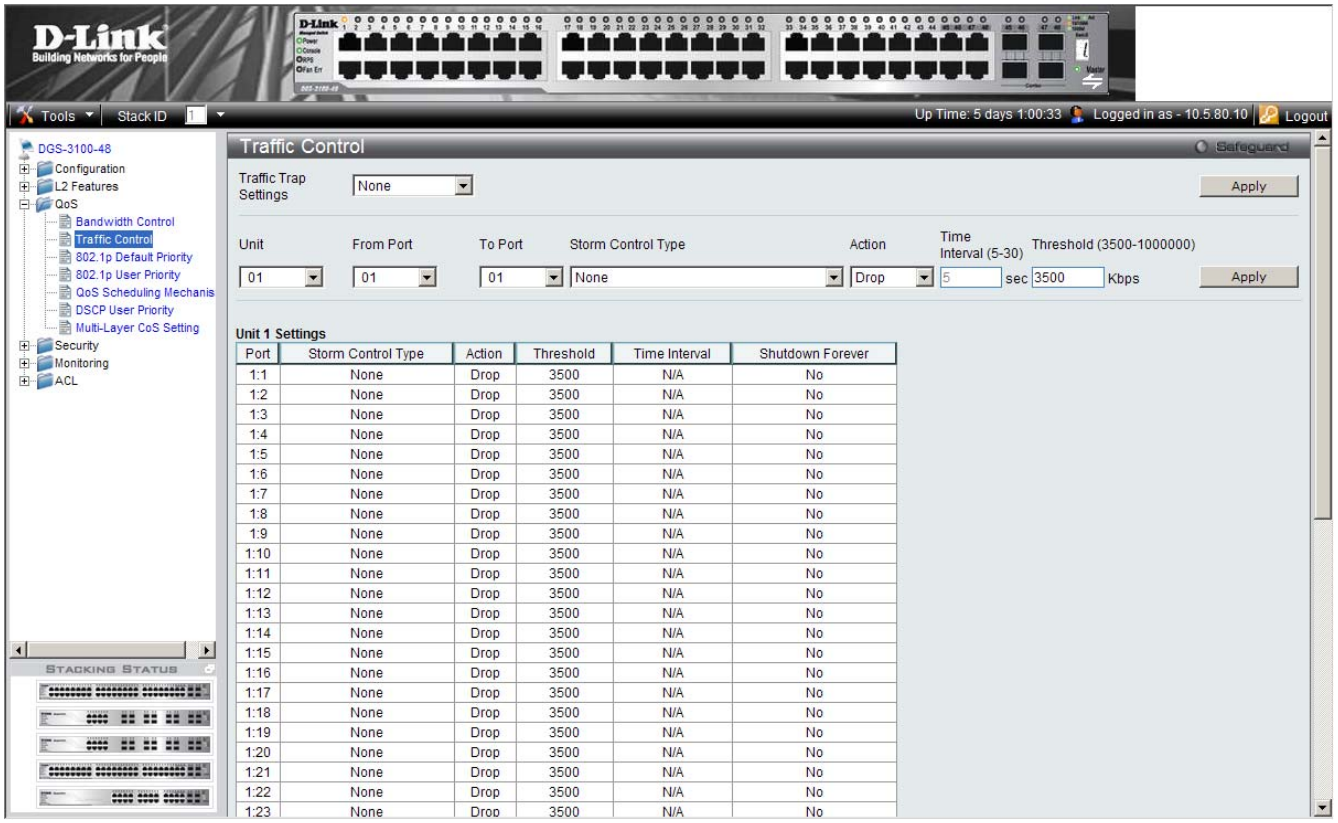


Figure 4-3 Traffic Control Settings Page

The Traffic Control Settings Page contains the following fields:

Field	Description
Traffic Trap Settings	Defines whether to send out a trap when a Traffic Storm occurs. The possible field values are: *None* — Do not send out traps when a Traffic Storm occurs. *Storm* Occurred — Send out traps (SNMP and Syslog) when a Traffic Storm occurs. These traps are sent only on ports on which the action is Shutdown.
Unit	Defines the stacking member for which the storm control parameters are displayed.
From Port	Defines from which port storm control is configureed.
To Port	Defines to which port storm control is configured.
Storm Control Type	Specifies the Broadcast mode currently enabled on the device. The possible field values are: *Broadcast Storm* *Broadcast and Multicast Storm* *Broadcast, Multicast and Unknown Unicast Storm*
Action	Indicates which storm action to perform if a Broadcast Storm occurs. The possible field values are:

Field	Description
	Drop — Discard the packets that exceed the threshold. *Shutdown* — Shut down the port that receives the storm traffic. A trap can be optionally sent. The administrator can reactivate this port.
Time Interval (5-30)	The time, in seconds, that the port counts the incoming traffic rate , in accordance to the storm control type.
Threshold (3500-1000000)	Indicates the maximum rate (kilobits per second) at which 'storm' packets are forwarded. The range is 3500 -1,000,000. The default value is 3,500.

2. Define the Unit, From Port, To Port, Storm Control Type, State, and Threshold fields.
3. Click Apply. The storm control settings are configured, and the device is updated.

Mapping Ports to Packet Priorities

The *802.1P Default Priority Page* provides traffic classification. by assigning priority values per port. The priority value is assigned when packet arrives to a port with an empty priority tag.

1. Click **QoS > 802.1p Default Priority**. The *802.1P Default Priority Page* opens:

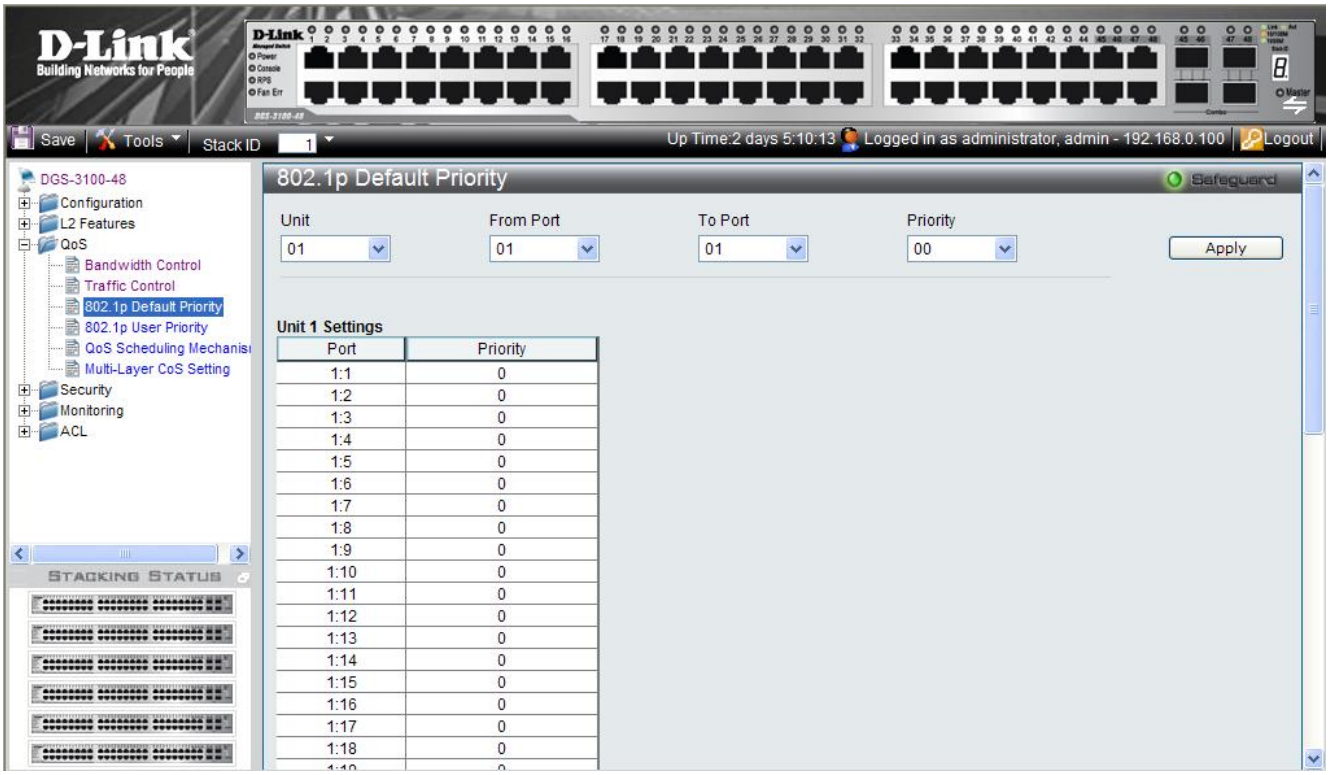


Figure 4-4 802.1P Default Priority Page

The 802.1P Default Priority Page contains the following fields:

Field	Description
Unit	Defines the stacking member for which the port packet priorities are displayed.
From Port	Defines the starting port for which the port packet priorities are defined.
To Port	Defines the ending port to which the port packet priorities are defined.
Priority	Defines the priority assigned to the port. The field range is 00-07, where 00 is the lowest priority and 07 is the highest priority.

2. Define the Unit, From Port, To Port, Prioirity fields.
3. Click Apply. Ports are mapped to packet priorities, and the device is updated.

Mapping Priority to Classes (Queues)

The *802.1P User Priority Page* allows network managers to assign priority tags to classes (queues). If a network manager defines a priority of 01 to Class 3, all packets arriving with an assigned value of 01 are sent to class (queue) 3.

The default mapping is:

- Priority 0. 3 is assigned to Q0. This is the lowest priority queue.
- Priority 1, 2 is assigned to Q1.
- Priority 4, 5 is assigned to Q2.
- Priority 6, 7 is assigned to Q3. This is the highest priority queue.

To map priority to queues:

1. Click **QoS > 802.1p User Priority**. The *802.1P User Priority Page* opens:

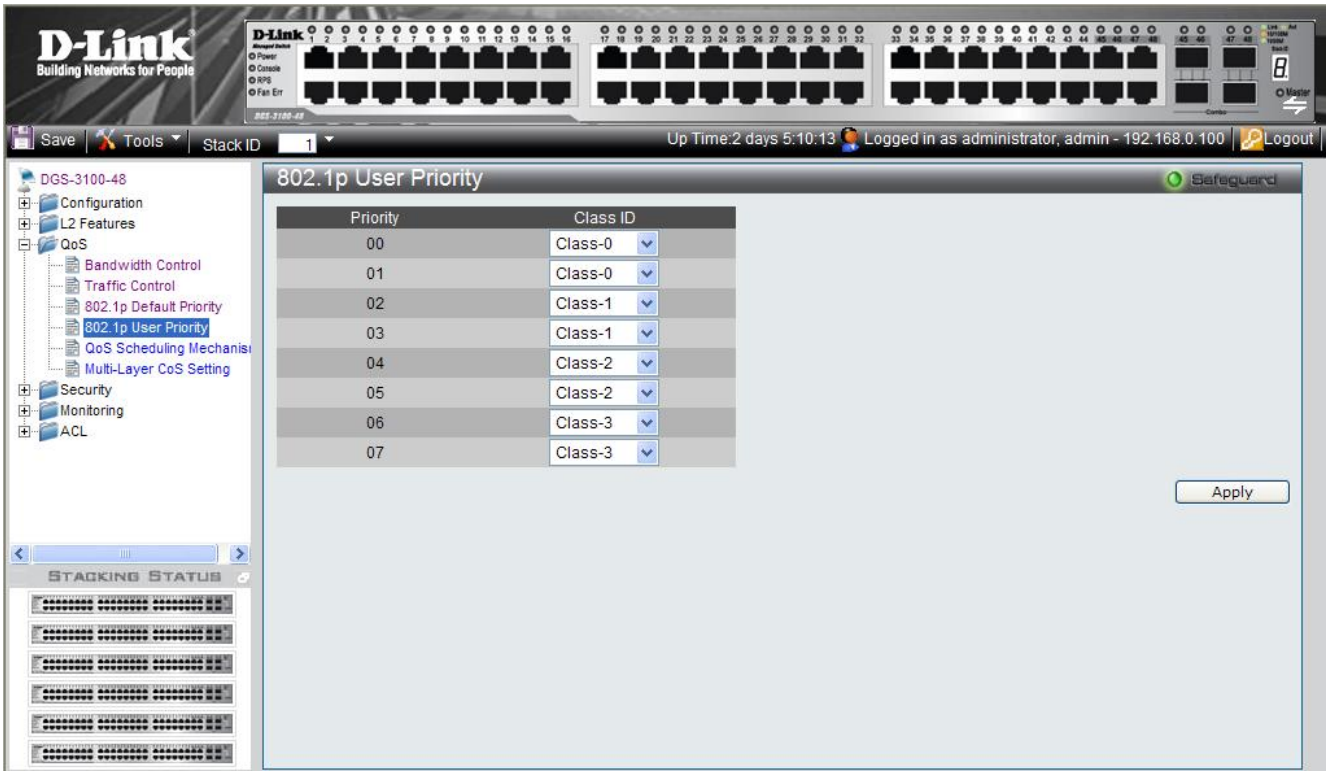


Figure 4-5 802.1P User Priority Page

The 802.1P User Priority Page contains the following fields:

Field	Description
Priority	Indicates the packet priority that is assigned to the queue.
Class ID	Defines the class (queue) that is assigned to the priority. Class 0 is the lowest priority queue, whereas Class 3 is the highest.

2. Define the queuing priority for 00 – 07 in the *Class ID* fields.
3. Click Apply. The User priority tags are assigned to classes, and the device is updated.

Configuring QoS Scheduling Mechanism

The *QoS Scheduling Mechanism Page* contains fields for defining the QoS scheduling forwarding scheme. To define the QoS scheduling mechanism:

1. Click **QoS > QoS Scheduling Mechanism**. The *QoS Scheduling Mechanism Page* opens:

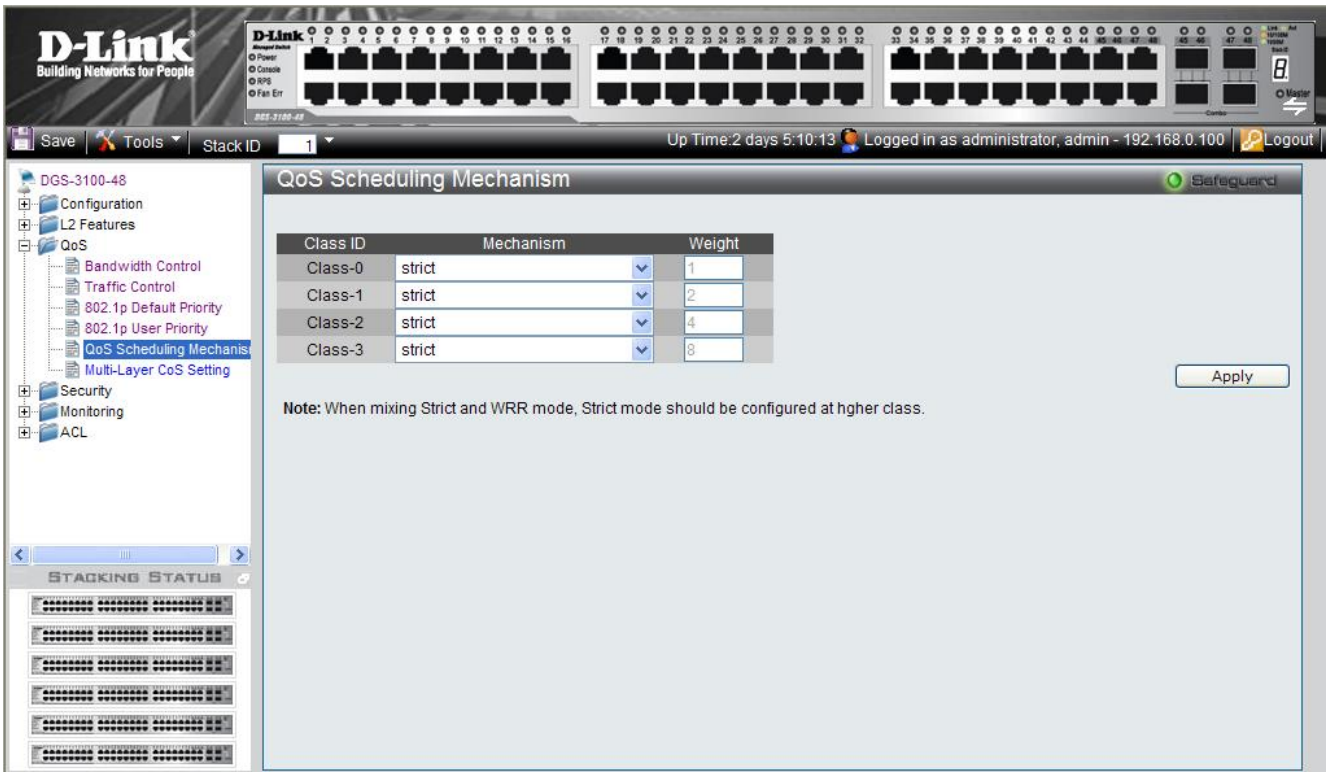


Figure 4-6 QoS Scheduling Mechanism Page

The QoS Scheduling Mechanism Page contains the following fields:

Field	Description
Class ID	Indicates the Class/queue for which the scheduling method is defined.
Mechanism	Defines the QoS class/queue scheduling method. The possible field values are: *Strict* — Specifies whether traffic scheduling is based strictly on the queue priority. Traffic with the highest Class of Service is the first traffic. That is, the highest class of service will finish before other queues empty. *Round Robin* — Assigns WRR weights to queues. This field is enabled only for queues in WRR queue mode. If a queue is set to 0 weight, the queue is not operational and is effectively closed. Each queue has a weight range, queues 0-3 have the range 0-15 When mixing Strict and WRR mode, Strict mode should be configured at higher class.(Class 3 and Class 2)
Weight	Assigns the specific WRR value to the Queue. The weight value range is 0-15.

2. Select the Class IDs in the *Mechanism* field.
3. Click Apply. The QoS Scheduling Mechanism is configured, and the device is updated.

Defining DSCP User Priority

The *DSCP User Priority Page* contains fields for mapping DSCP settings to traffic queues. For example, a packet with a DSCP tag value of 3 can be assigned to queue 2.

To map priority tags to classes:

1. Click **QoS > DSCP User Priority**. The *DSCP User Priority Page* opens:

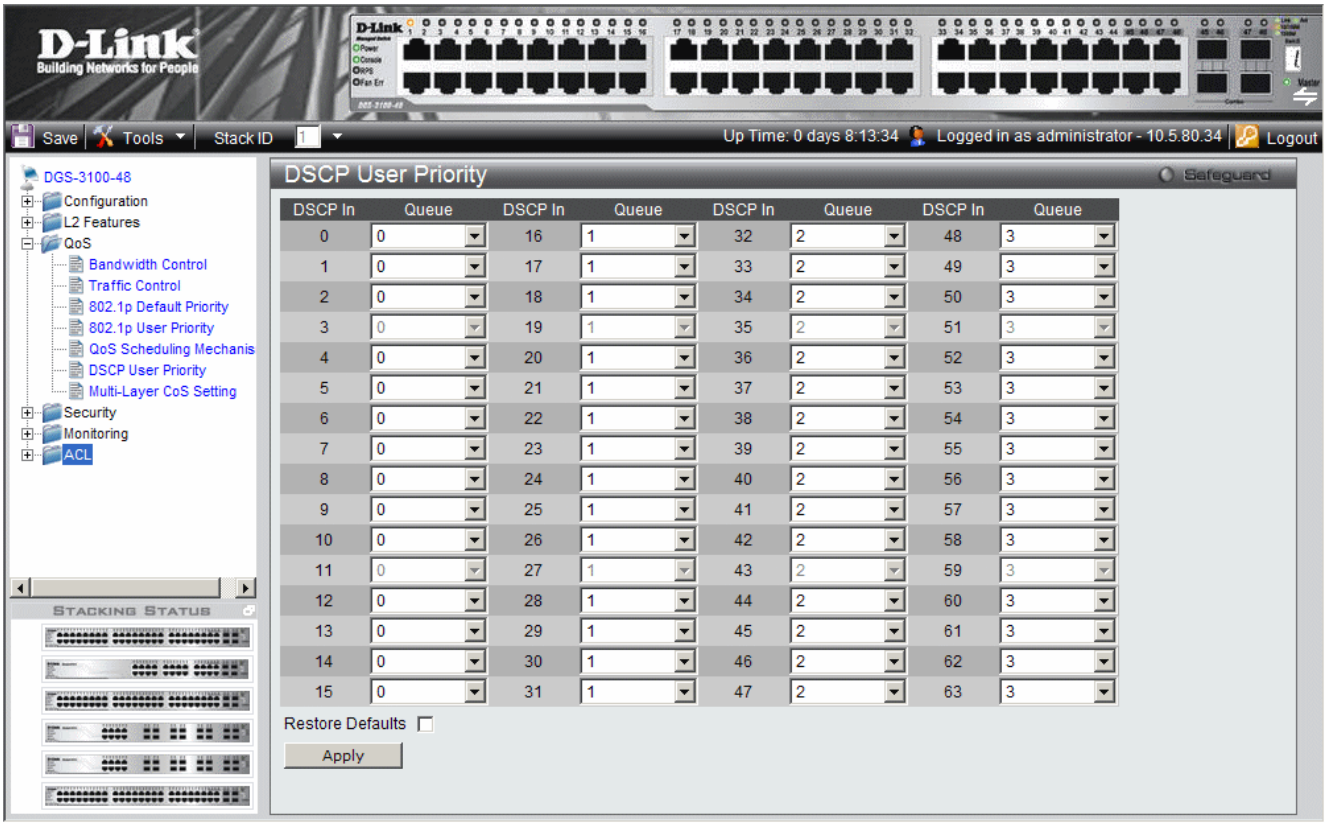


Figure 4-7 DSCP User Priority Page

The *DSCP User Priority Page* contains the following fields:

Parameter	Description
DSCP In	Displays the incoming packet's DSCP value.
Queue	Specifies the traffic forwarding queue to which the DSCP priority is mapped. Four traffic priority queues are supported.
Restore Defaults	Restores the Switch factory defaults for mapping DSCP values to a forwarding queue.

2. Modify the Queue values.
3. Click Apply. The DSCP mapping configuration is modified and the Switch is updated.

Defining Multi-Layer CoS Settings

For network administrators wanting to configure Multi Layer CoS settings, implementation in the switch is done via the Access Control List. Hence, the *Multi-Layer CoS Setting Page* has two hyperlinks; one to the Access Profile List, which enables the utilization of existing ACL rules to perform traffic classification, and the other to the ACL Configuration Wizard, which enables network administrators to create new ACL traffic classification rules. To define CoS/QoS settings:

1. Click **QoS > Multi-Layer CoS Settings**. The *Multi-Layer CoS Setting Page* opens:

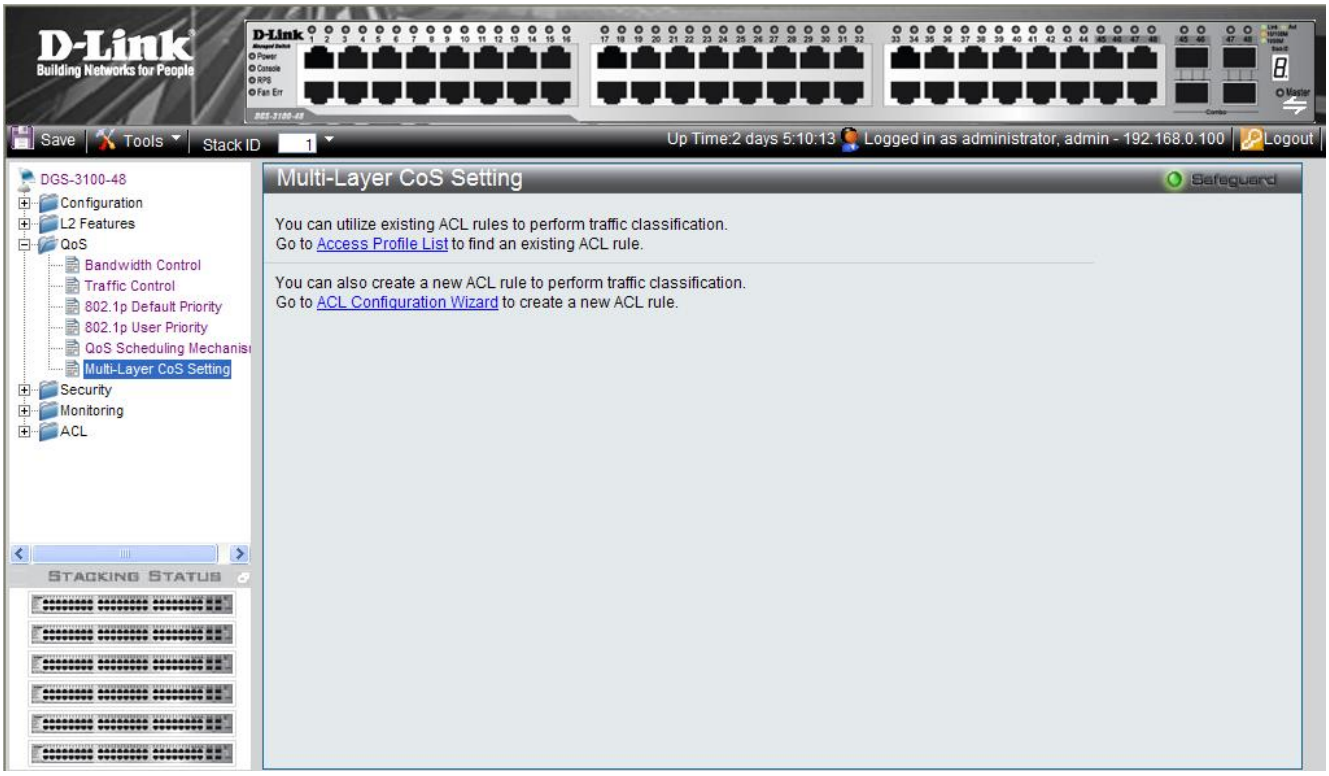


Figure 4-8 Multi-Layer CoS Setting Page

The Multi-Layer CoS Setting Page contains the following links:

- Access Profile List
- ACL Configuration Wizard

2. Click the desired link. The relevant page opens (see Defining Access Profile Lists).

5

SECURITY FEATURES

This section contains information for enabling and configuring device security including user accounts.

- Configuring Safeguard Engine
- Configuring Trust Host
- Configuring Port Security
- Configuring Guest VLANs
- Configuring Port Authentication 802.1X
- Defining EAP Forwarding Settings
- Configuring Secure Socket Layer Security
- Configuring Secure Shell Security
- Defining Application Authentication Settings

Configuring Safeguard Engine

The *Safeguard Engine Page* allows network administrators to set network alarms to protect the CPU from attacks, based on *rising* and *falling threshold* levels of Broadcasts and CPU Utilization. The Safeguard mechanism immediately implements Broadcast Storm Control with a low threshold in order to hold the attack and release the CPU resources. To enable the safeguard engine:

1. Click **Security > Safeguard Engine**. The *Safeguard Engine Page* opens:

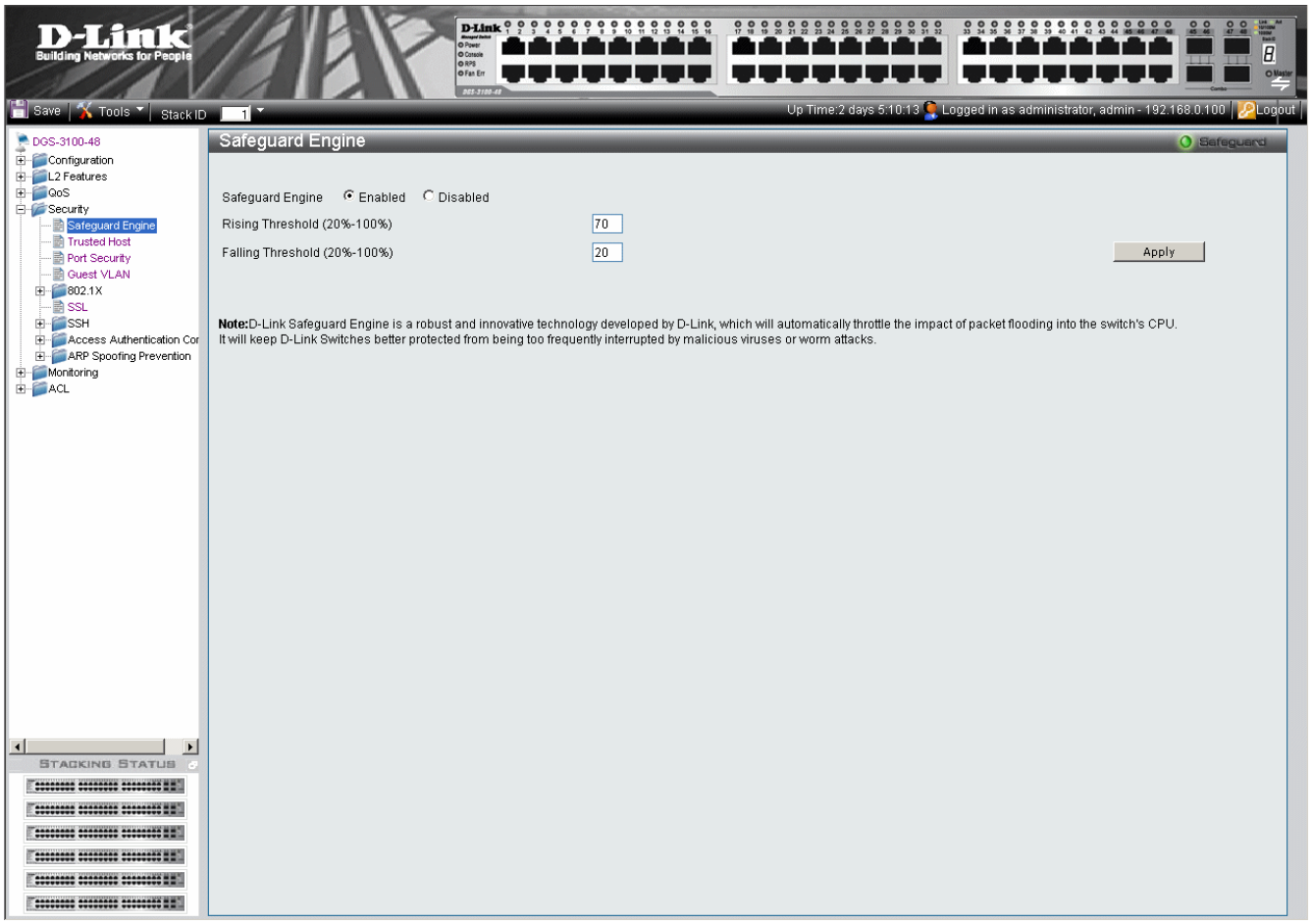


Figure 5-1 Safeguard Engine Page

The Safeguard Engine Page contains the following field:

Field	Description
Safeguard Engine	Indicates if the safeguard engine is enabled on the device. The possible field values are: *Enabled* — Enables the safeguard engine on the device. This is the default value. *Disabled* — Disables the safeguard engine on the device.
Rising Threshold (20%-100%)	Indicates the rising CPU Utilization thresholds enabling Safegard .The possible field range is between 20%-100%. The default value is 70%.
Falling Threshold (20%-100%)	Indicates the falling CPU Utilization thresholds disabling Safeguard. The possible field range is between 20%-100%. The default value is 20%.

2. Set the safeguard engine status in the *Safeguard Engine* field.
3. Define the Rising Threshold and Falling Threshold fields.
4. Click Apply. The Safeguard Engine is enabled, and the device is updated.

Configuring Trust Host

The *Trusted Host* Page enables network managers to apply restrictions on managing the device from remote stations. Network managers can configure up to 30 remote stations. Only those stations that are included in this list may manage the device. Ensure that the IP address from which the device is currently being configured is included to prevent disconnection. To enable Trust Host:

1. Click **Security > Trusted Host**. The *Trusted Host* **Page** opens:

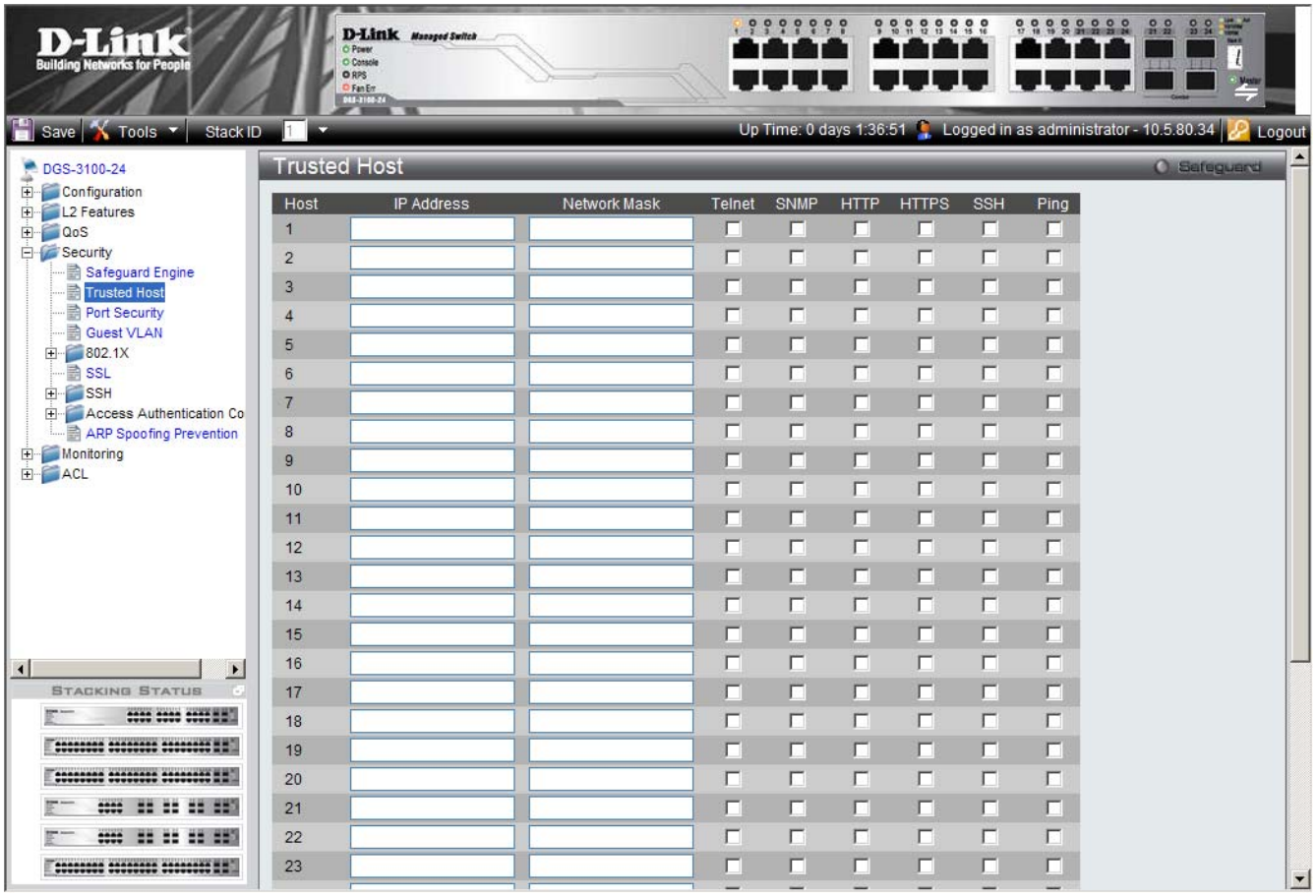


Figure 5-2 Trusted Host Page

The Trusted Host Page contains the following fields:

Field	Description
IP Address (1-30)	Defines the management station IP address from which the device can be managed.
Network Mask (1-30)	Defines the management station IP Subnet Mask from which the device can be managed.
Telnet	If selected, permits Telnet access to be used for management access to the device.
SNMP	If selected, permits SNMP access to be used for management access to the device.
HTTP	If selected, permits HTTP access to be used for management access to the device.
HTTPS	If selected, permits HTTPS (Secure HTTP) access to be used for management access to the device.
SSH	If selected, permits SSH (Secure Telnet) access to be used for management access to the device.
Ping	If selected, permits the host to ping the device.

2. Define the IP 1-30 Address fields and Subnet Mask to define the remote management stations.
3. Click Apply. The management stations are defined, and the device is updated.
4. To remove a station from the Trusted Hosts list, clear the IP Address field and click Apply.

Configuring Port Security

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. The MAC addresses can be dynamically learned or statically configured. Locked port security monitors both received and learned packets that are received on specific ports. Access to the locked port is limited to users with specific MAC addresses. These addresses are either manually defined on the port, or learned on that port up to the point when it is locked. When a packet is received on a locked port, and the packet source MAC address is not tied to that port (either it was learned on a different port, or it is unknown to the system), the protection mechanism is invoked, and can provide various options. Unauthorized packets arriving at a locked port are either:

- Discarded with no trap
- Discarded with a trap

Locked port security also enables storing a list of MAC addresses in the configuration file. The MAC address list can be restored after the device has been reset. To define port security:

1. Click **Security > Port Security**. The *Port Security Page* opens:

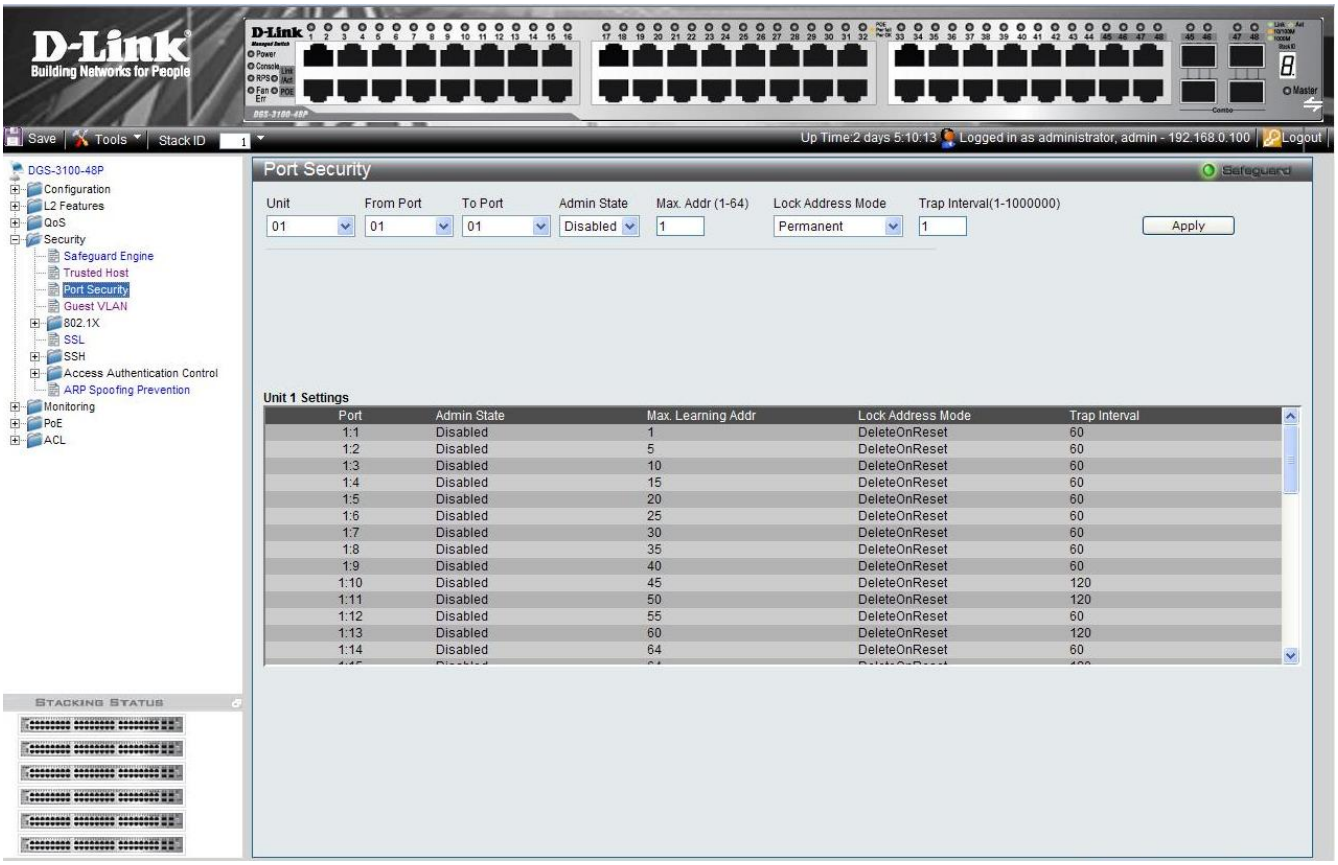


Figure 5-3 Port Security Page

The Port Security Page contains the following fields:

Field	Description
Unit	Displays the stacking member's ID for which the port security parameters are displayed.
From Port	Indicates the port number from which the port security parameters are displayed.
To Port	Indicates the port number to which the port security parameters are displayed.
Admin State	Indicates if port security on the device. The possible field values are: *Enable* — Indicates that port security is enabled on the device. *Disable* — Indicates that port security is disabled on the device. This is the default value.

Field	Description
Max Address(1-64)	Defines the number of MAC addresses. The field value is 1-64. The field default is 1.
Lock Address Mode	The *Lock Address Mode* allows network administrators to limit the number of MAC addresses learned on a port, or to stop learning MAC address completely. Ports can be assigned a MAC address which is not aged out nor is the MAC address relearned, therefore *Locking* the port to the MAC address. After the port is locked, the all the dynamic MAC addresses associated with the port are deleted. The possible field values are: *Permanent* – Learns up to the maximum number of dynamic addresses allowed on the port. The learned addresses are not aged out or relearned on other port for as long as the port is locked. *Delete on Reset* – Deletes the current dynamic MAC addresses associated with the port. Learn up to the maximum addresses allowed on the port (this number is also configurable). Aging is disabled; the addresses are deleted on reset. *Delete on Timeout* – Deletes the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Re-learned MAC addresses and address aging out are also enabled. The MAC addresses are deleted when the device is reset and on when the address is aged out.
Trap Interval (1-1000000)	Indicates the amount of time (seconds) between Port Security traps sent to the interface. The possible field range is 1- 1000000 seconds. The field default is 10 seconds.
Port	Displays the specific port number.
Max Learning Addr	Indicates the number of MAC addresses which learned on the port.

2. Define the Unit, From Port, To Port, Max Address (1-64), Admin State, Lock Address Mode and Trap Interval (1-1000000) fields.
3. Click

Port security is enabled, and the device is updated.

Configuring Guest VLANs

Guest VLANs provide limited network access to authorized ports. If a port is denied network access via port-based authorization, but the Guest VLAN is enabled, the port receives limited network access. For example, a network administrator can use Guest VLANs to deny network access via port-based authentication, but grant internet access to unauthorized users. To define Guest VLANs:

1. Click **Security > Guest Vlan**. The *Guest VLAN Page* opens:

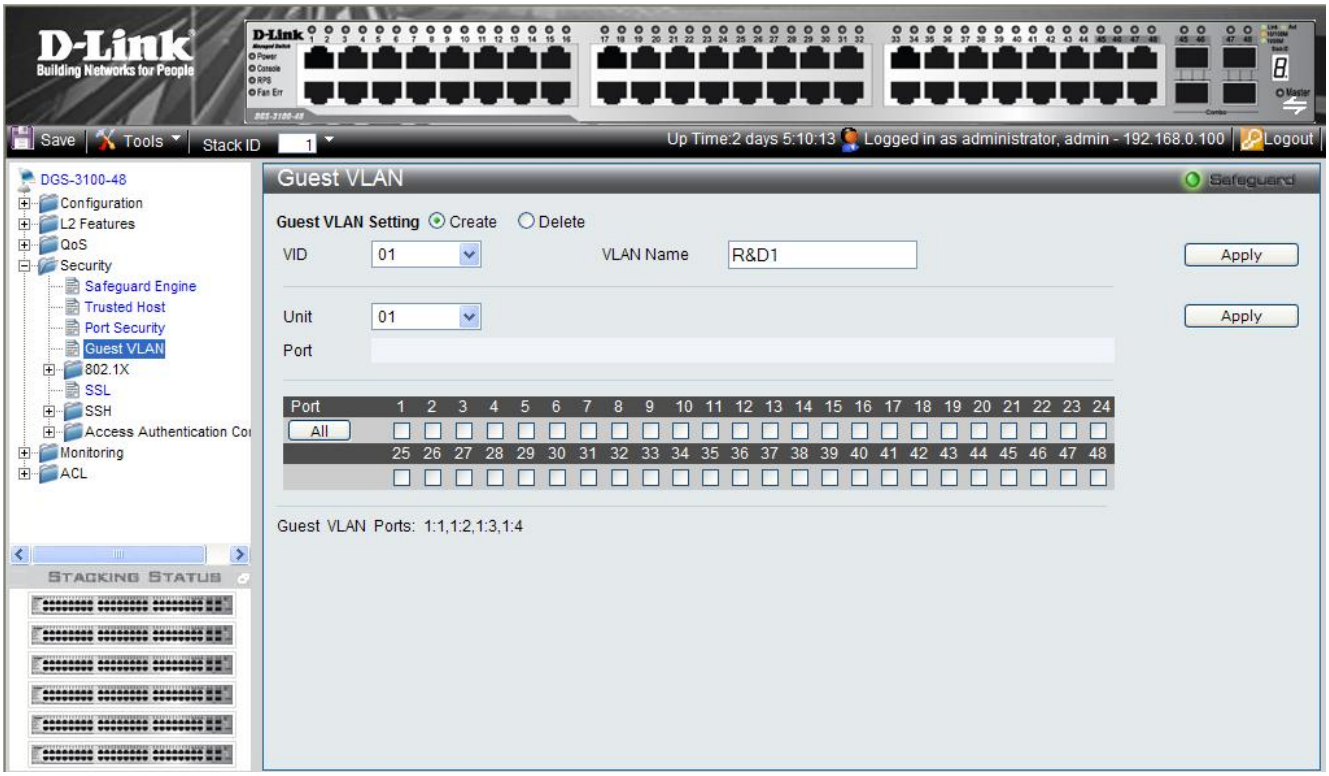


Figure 5-4 Guest VLAN Page

The Guest VLAN Page contains the following fields:

Field	Description
VID	Defines the VLAN ID on which the Guest VLAN is created.
VLAN Name	Defines the user-defined VLAN name assigned to the guest VLAN.
Unit	Defines the stacking member for which the Guest VLAN parameters are displayed.
Port	Defines the ports included in the Guest VLAN.

2. Define the VLAN ID in the *VID* field.
3. Define the VLAN name in the *VLAN Name* field
4. Select the stacking member which the Guest VLAN parameters are displayed in the *Unit* field.
5. Select the ports to be included in the Guest VLAN in the *Port* checkbox field. The selected ports appear in the *Port* field.
6. Click Add. The Guest VLAN is added, and the system is updated.

Configuring Port Authentication 802.1X

Port-based authentication authenticates users on a per-port/per mac basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the RADIUS server using the *Extensible Authentication Protoco*l (EAP). The 802.1x Access Control protocol consists of the following vital components which stabilize Access Control Security:

Component	Description
Authenticators	The Authenticator is an intermediary between the Authentication Server and the Client. The authenticator: Requests certification information via the Client (EAPOL packets). The EAPOL packets are the only information allowed to pass between supplicants and the authentication server until the authenticator is granted system access. Verifies the information gathered from the Client with the Authentication Server, and relays the information to the Client.
Supplicants/Clients	Specifies the host connected to the authenticated port requesting to access the system services.
Authentication Server	Specifies the server that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services. The Authentication Server is a remote device connected to the Client network and Authenticator. The Authentication Server must have RADIUS Server application enabled and configured. Clients connected to a port on the Switch must be authenticated by the Authentication Server before accessing any system services. The Authentication Server certifies the client's identity attempting to access the network by exchanging secure information between the RADIUS server and the Client.
Dynamic VLAN Assignment (DVA)	Assigns users to VLANs during the RADIUS server authentication. When a user is authenticated by the RADIUS server, the user is automatically joined to the VLAN configured on the RADIUS server. The VLANs that cannot participate in the DVA are: – A Dynamic GVRP-created VLAN – A Voice VLAN – A Default VLAN – A Guest VLAN

Port-based authentication creates two access states:

State	Description
Controlled Access	Permits communication between the supplicant and the system, if the supplicant is authorized.
Uncontrolled Access	Permits uncontrolled communication regardless of the port state.

To enable the 802.1X:

1. Click **Security > 802.1X Setting**. The *802.1X Setting Page* opens:

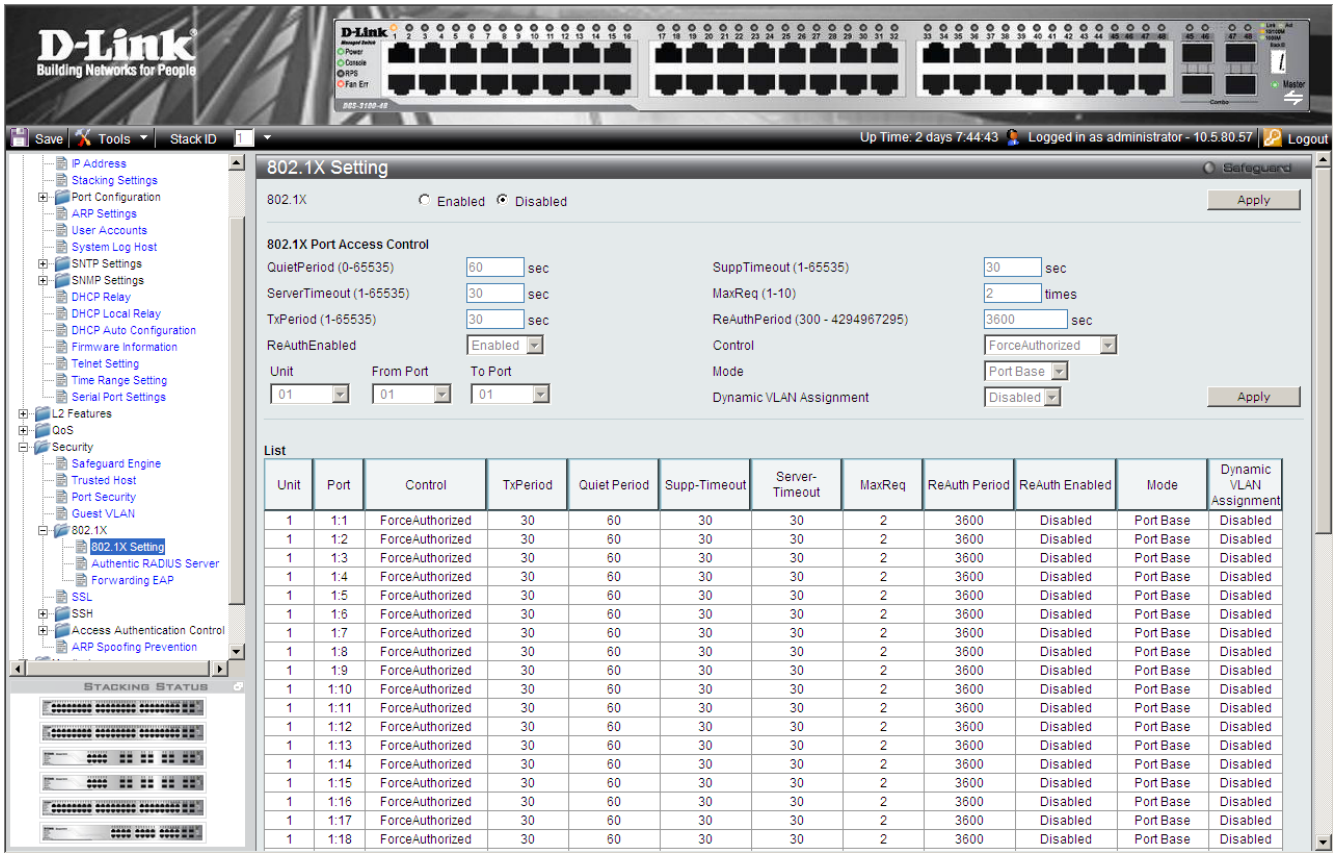


Figure 5-5 802.1X Setting Page

The 802.1X Setting Page contains the following fields:

Field	Description
802.1X	Indicates if 802.1X is enabled on the device. The possible field values are: *Enabled* — Enables 802.1X on the device. *Disabled* —Disables 802.1X on the device. This is the default value.
QuietPeriod (0-65535) sec	Indicates the number of seconds that the device remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field default is 60 seconds.
SuppTimeout (1-65535) sec	Indicates the amount of time that lapses before EAP requests are resent to the supplicant. The field value is in seconds. The field default is 30 seconds.
ServerTimeout (1-65535) sec	Defines the amount of time that lapses before the device re-sends a request to the authentication server. The field value is specified in seconds. The field default is 30 seconds.
MaxReq (1-10) times	Displays the total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries.
TxPeriod (1-65535) sec	Defines the amount of time (in seconds) that lapses before EAP requests are resent. The field default is 30 seconds.
ReAuthPeriod (300 - 4294967295) sec	Displays the time span (in seconds) in which the selected port is re-authenticated. The field default is 3600 seconds.
ReAuthEnabled	Indicates if ports/MAC address can be re-authenticated after the port/MAC address authentication has timed out. The possible field values are:

Field	Description
	Enabled — Enables re-authenticating the port or MAC addresses after the port or MAC address authentication has timed out. This is the default value. *Disabled* — Disables re-authenticating the port or MAC addresses after the port or MAC address authentication has timed out.
Control	Indicates the host status. If there is an asterisk (*), the port is either not linked or is down. The possible field values are: *ForceUnauthorized* — Indicates that either the port control is Force Unauthorized and the port link is down, or the port control is Auto but a client has not been authenticated via the port. *ForceAuthorized* — Indicates that the port control is Forced Authorized, and clients have full port access. *Auto* — Indicates that the port control is Auto. The user has to authenticate and get full access..
Unit	Indicate the stacking member for which the 802.1X parameters are defined.
From Port	Indicates the first port for which the 802.1X parameters are defined.
To Port	Indicates the last port for which the 802.1X parameters are defined.
Mode	Indicates the 802.1X mode enabled on the device. The possible field values are: *Port Base* — Enables 802.1X on ports. This is the default value. *MAC Base* — Enables 802.1xon MAC addresses.
Dynamic VLAN Assignment	Indicates if Dynamic VLAN Assignment is enabled on the device. The possible field values are: • *Enabled* — Enables Dynamic VLAN Assignment on the device. • *Disabled* —Disables Dynamic VLAN Assignment on the device. This is the default value.

2. Enable or disable the 802.1X status in the *802.1X* field.
3. Define the *Mode* field.
4. In the *802.1X Port Access Control* section, define the fields.
5. Set the *ReAuthEnabled* field and the *Control* fields.
6. Set the values in the *Unit, From Port,* and *To Port* fields.
7. Click Apply. The 802.1x Access Control is configured, and the device is updated.

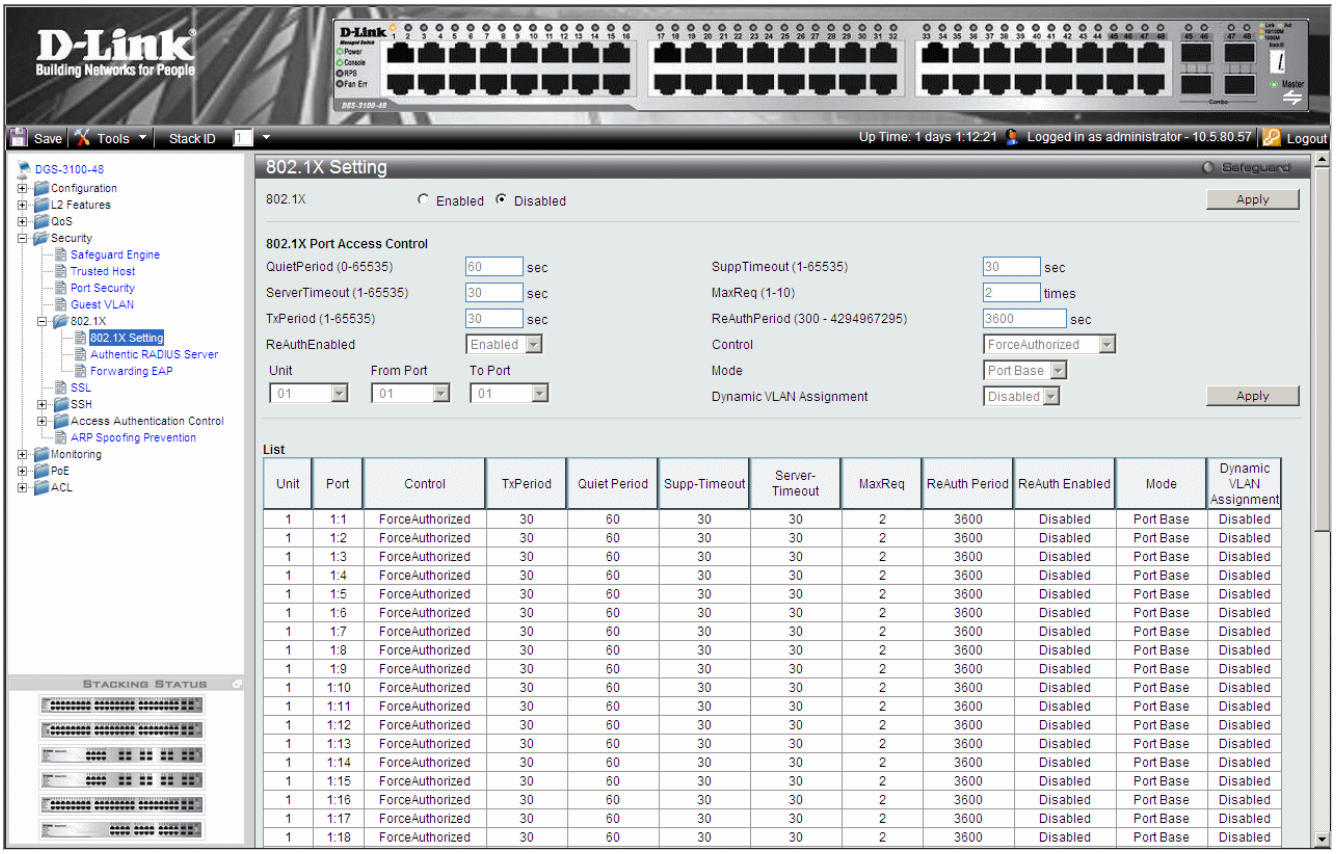
MAC Authentication (MAC-Based MAC Access Control)

1. MAC Authentication is configured in DGS-3100 series via '802.1x Setting' WEB page.
2. This functionality enables the user to allow specific MAC address to enter the switch while rejecting the unauthorized MAC addresses.
3. The database of the authorized MAC addresses resides in a Radius Server**.**

NOTE: MAC-based authentication doesn't require 802.1X client enabled.

To enable MAC Authentication:

1. Click **Security > 802.1X Setting**. The *802.1X Setting Page* opens:



The *802.1X Setting Page* contains the following fields:

Field	Description
802.1X	Indicates if 802.1X is enabled on the device. The possible field values are: *Enabled* — Enables 802.1X (and MAC Authentication) on the device. *Disabled* —Disables 802.1X on the device. This is the default value.
QuietPeriod (0-65535) sec	Indicates the number of seconds that the device remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field default is 60 seconds.
SuppTimeout (1-65535) sec	Indicates the amount of time that lapses before EAP requests are resent to the supplicant. The field value is in seconds. The field default is 30 seconds.
ServerTimeout (1-65535) sec	Defines the amount of time that lapses before the device re-sends a request to the authentication server. The field value is specified in seconds. The field default is 30 seconds.
MaxReq (1-10) times	Displays the total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries.
TxPeriod (1-65535) sec	Defines the amount of time (in seconds) that lapses before EAP requests are resent. The field default is 30 seconds.
ReAuthPeriod (300 - 4294967295) sec	Displays the time span (in seconds) in which the selected port is re-authenticated. The field default is 3600 seconds.
ReAuthEnabled	Indicates if ports/MAC address can be re-authenticated after the port/MAC address authentication has timed out. The possible field values are:

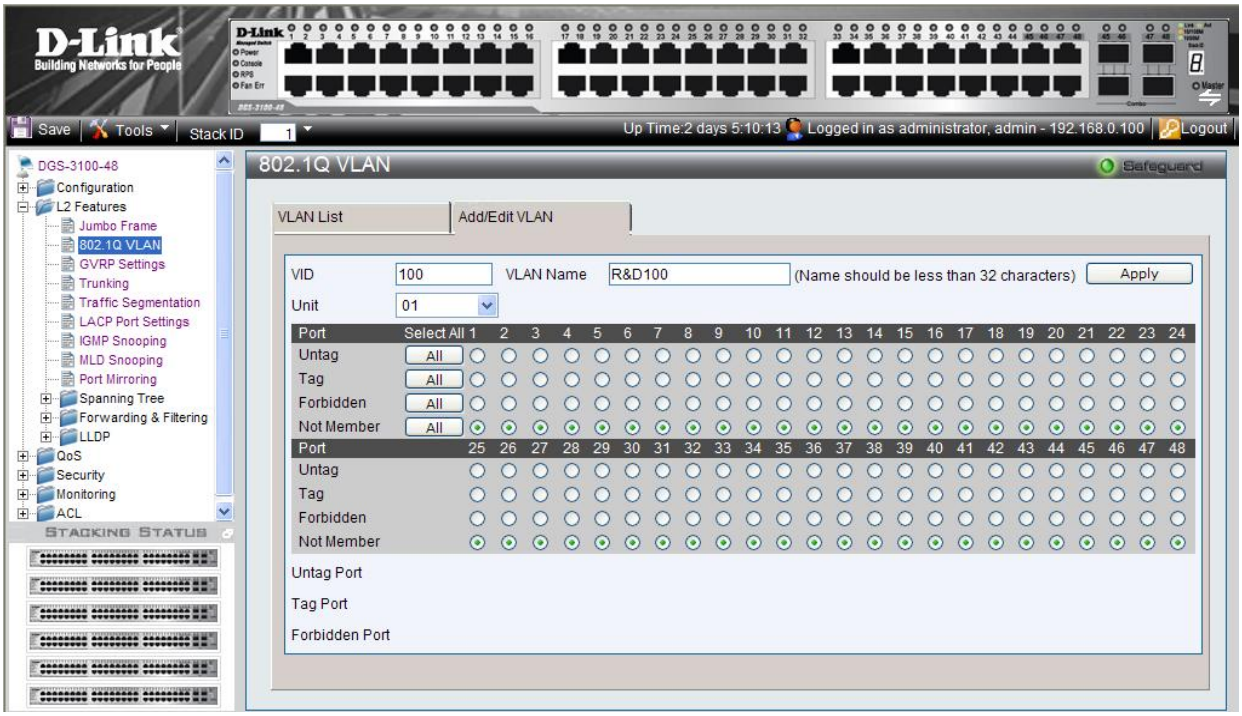
Field	Description
	Enabled — Enables re-authenticating the port or MAC addresses after the port or MAC address authentication has timed out. This is the default value. *Disabled* — Disables re-authenticating the port or MAC addresses after the port or MAC address authentication has timed out.
Control	Indicates the host status. If there is an asterisk (*), the port is either not linked or is down. The possible field values are: *ForceUnauthorized* — Indicates that either the port control is Force Unauthorized and the port link is down, or the port control is Auto but a client has not been authenticated via the port. *ForceAuthorized* — Indicates that the port control is Forced Authorized, and clients have full port access. *Auto* — Indicates that the port control is Auto and at least single client or single MAC has been authenticated via the port.
Unit	Indicate the stacking member for which the 802.1X parameters are defined.
From Port	Indicates the first port for which the 802.1X parameters are defined.
To Port	Indicates the last port for which the 802.1X parameters are defined.
Mode	Indicates the 802.1X mode enabled on the device. The possible field values are: *Port Base* — Enables 802.1X on ports. This is the default value. *MAC Base* — Enables 802.1X on MAC addresses.

2. Enable or disable the 802.1X status in the *802.1X* field.
3. Define the *Mode* field (MAC Base for MAC Authentication)
4. In the *802.1X Port Access Control* section, define the *time* fields.
5. Set the *ReAuthEnabled* field and the *Control* fields.
6. Set the values in the *Unit, From Port,* and *To Port* fields.
7. Click Apply. The MAC Authentication is configured, and the device is updated.
8. In order to activate MAC Based Authentication, the user should first enable 802.1X globally on the switch.
9. Then the user should define the port(s) that needs to be configured for MAC Authentication.
10. In the Mode control the user needs to select the ‘MAC Base‘option.
11. In addition to that the user needs to switch the ‘port Control’ to Auto and enable reauthentication
12. In order to complete the configuration the port must be member in the guest VLAN.

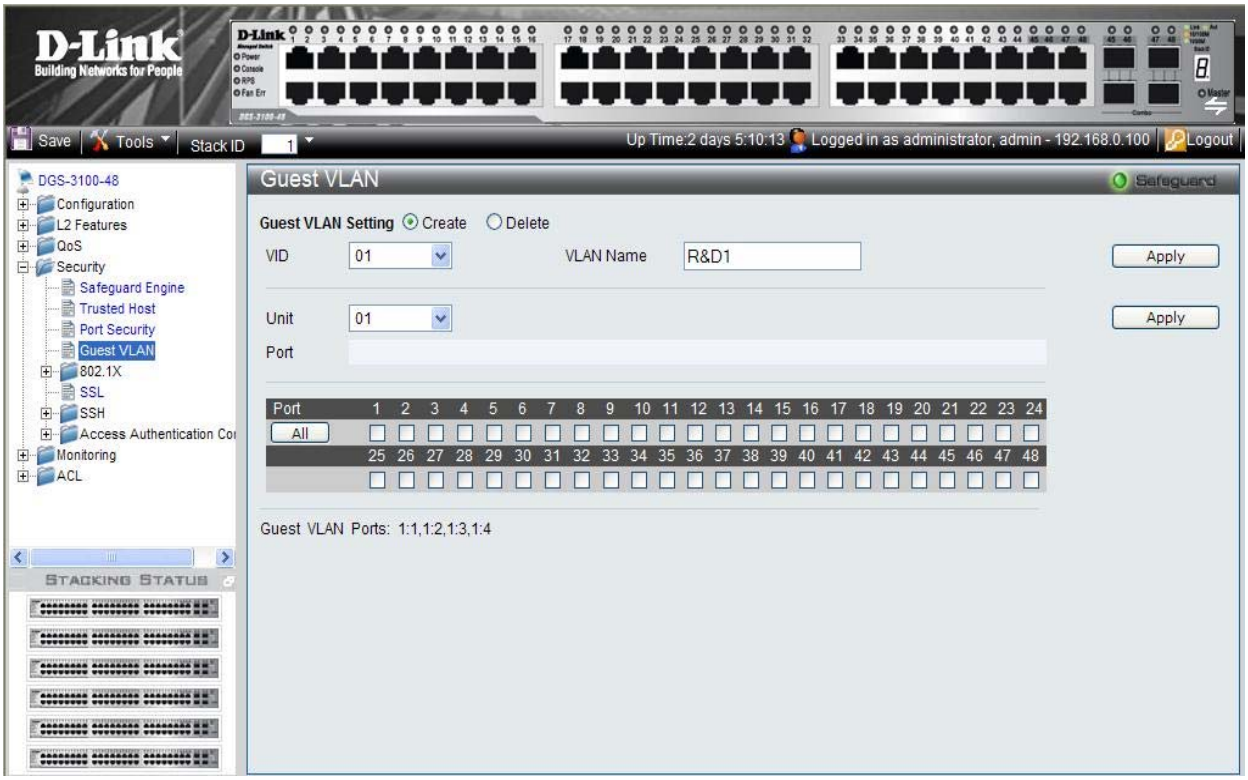
Configuring MAC Authentication (by using Guest VLAN, 802.1X and Radius pages)

This is the sequence of operatons required to configure MAC Authentication in DGS-3100 series.

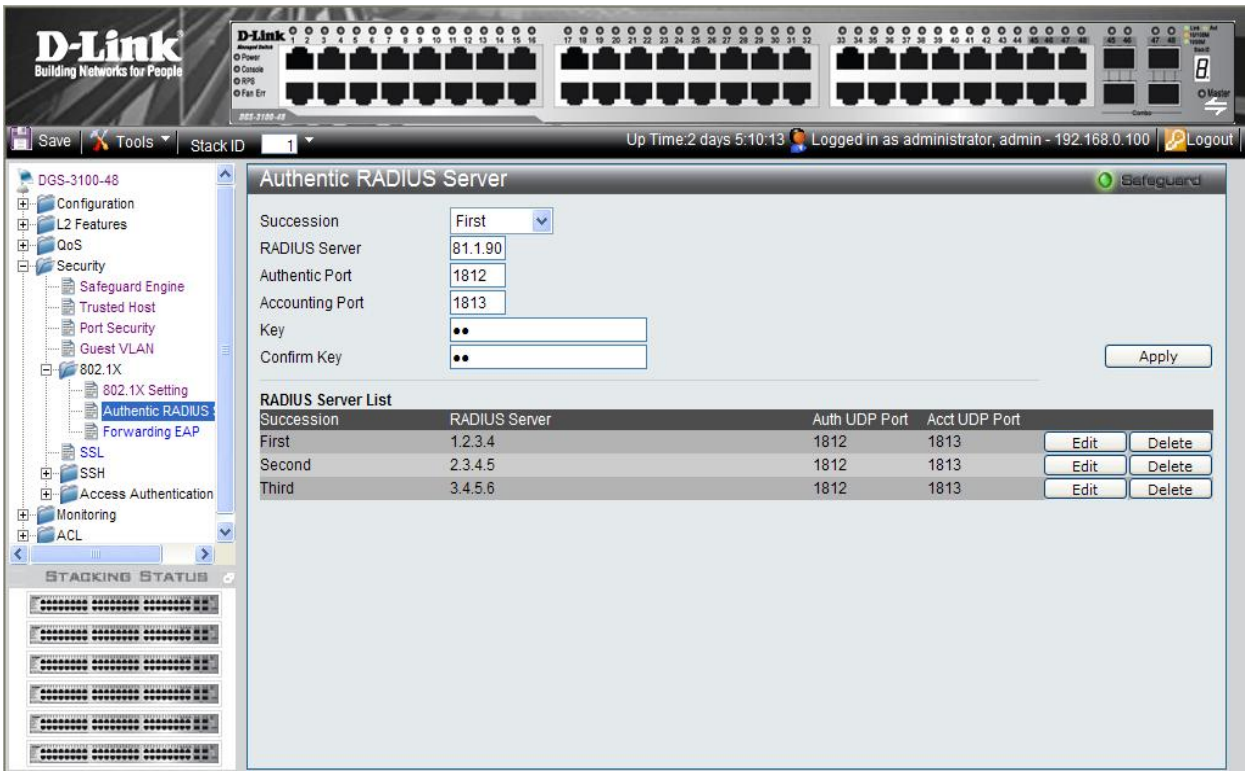
1. In order to configure a guest VLAN, the user is required to create a VLAN first, in the following example the user creates VLAN 100 via click **L2 Features > 802.1Q VLAN**. The *802.1Q VLAN page* opens**:**



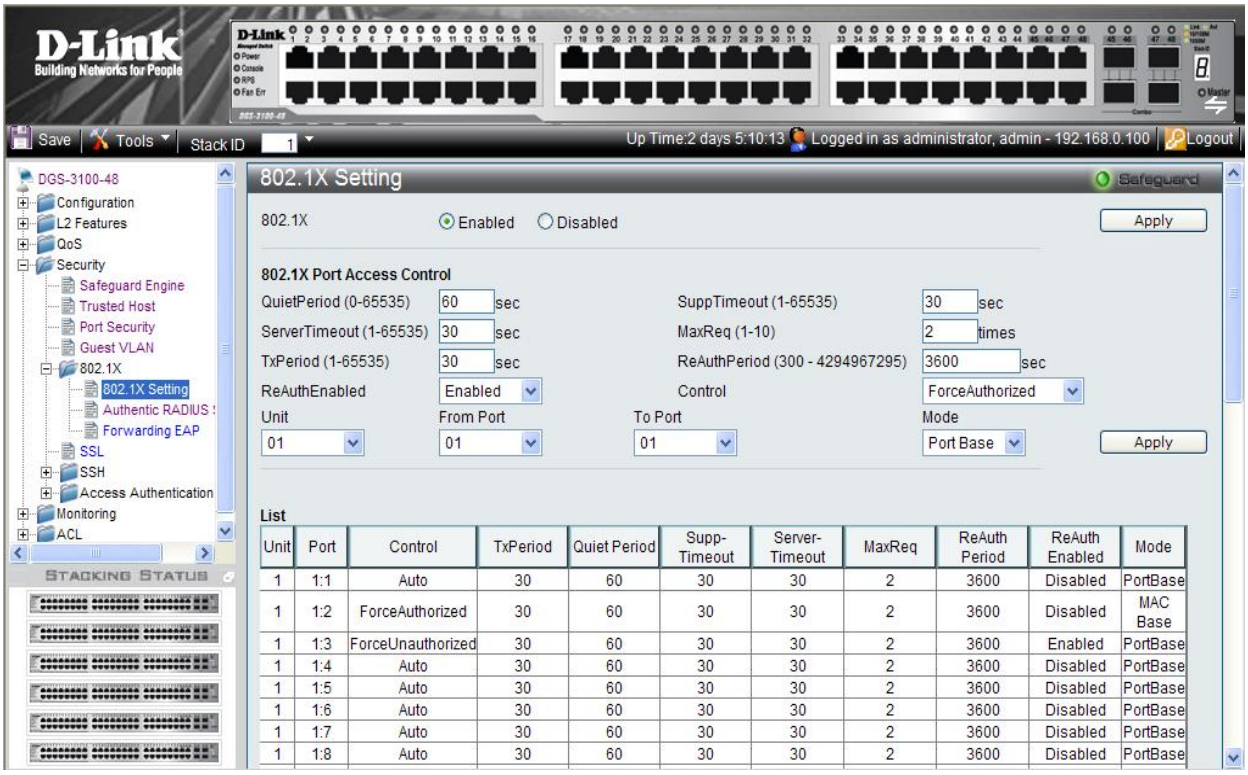
2. Assign ports to the Guest VLAN via click **Security > Guest** VLAN and according to the following example:



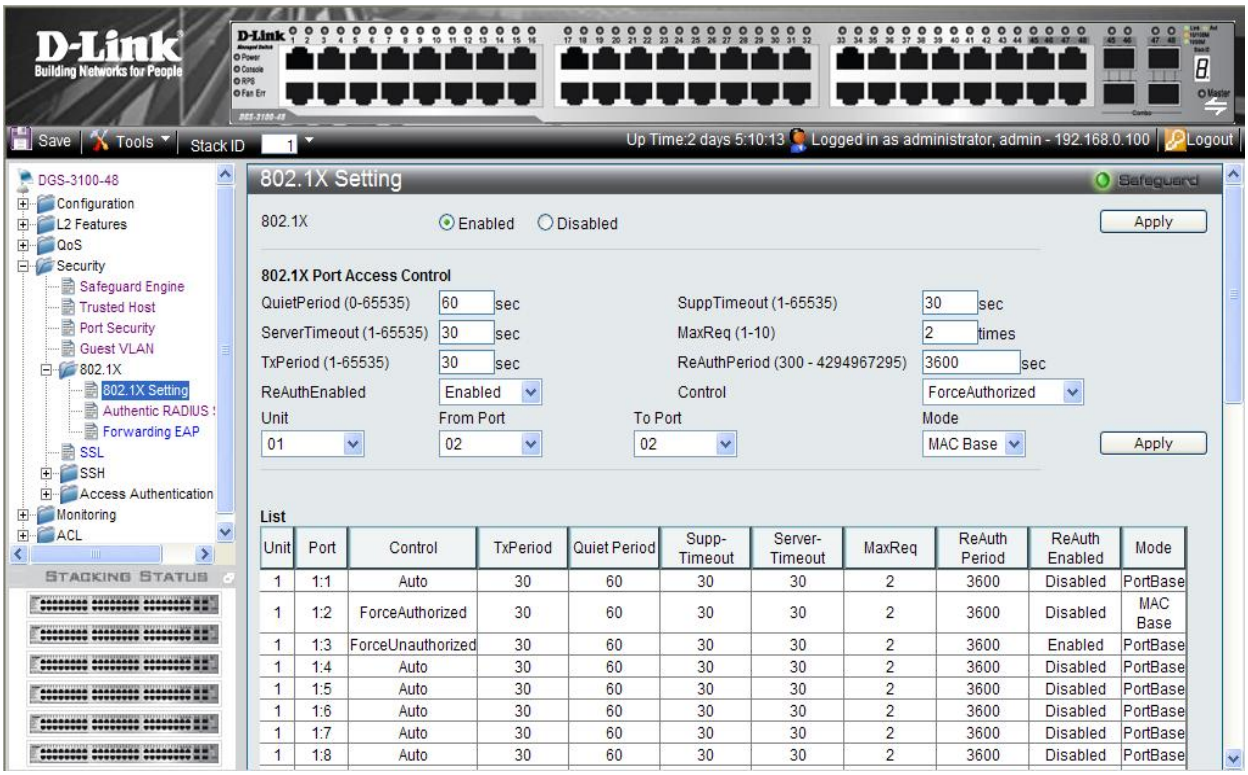
3. After the ports were assigned to the Guest VLAN, the user needs to configure a Radius Server that will hold the MAC Authentication database. This should be done via click **Security > 802.1X > Authentic RADIUS Server page** according to the example below.



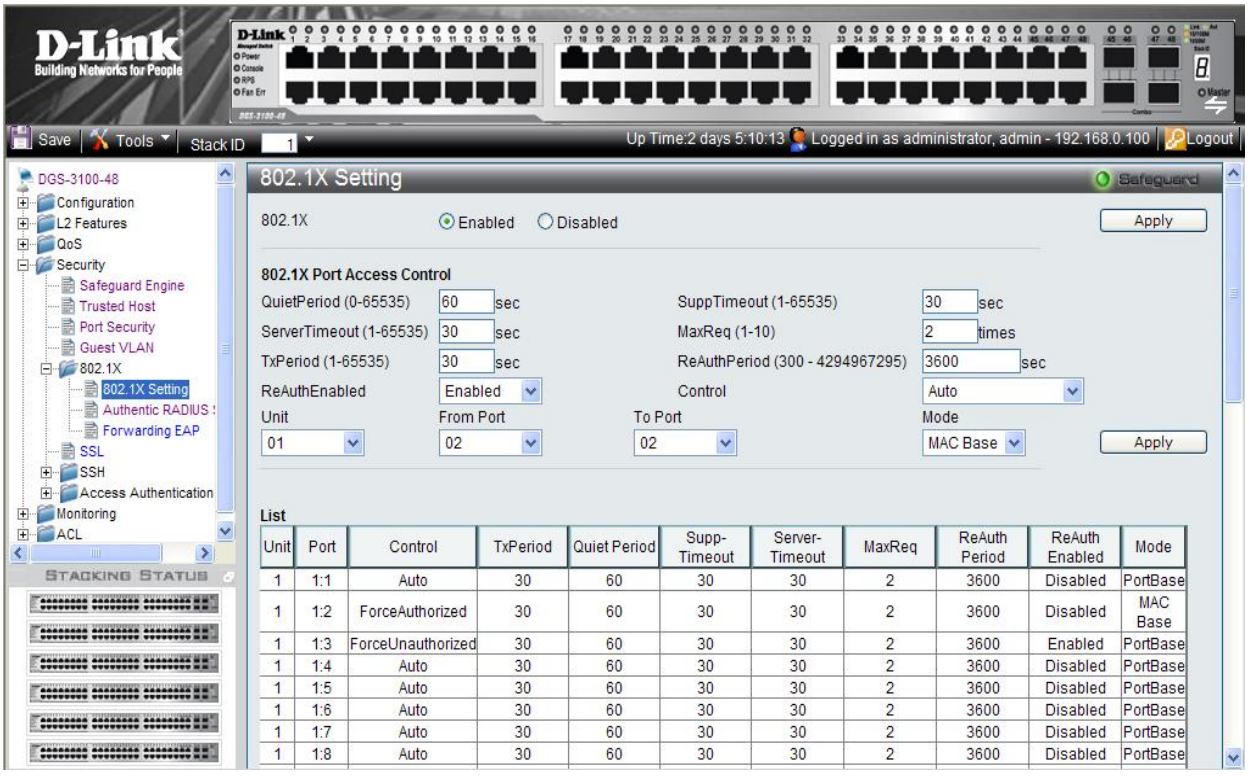
4. Click **Security > 802.1X > 802.1X Setting page**: first, 802.1x should be enabled globally and in the port level, 802.1x Control should be configured as 'ForceAuthorized**'.**



5. The second step on **Security > 802.1X > 802.1X Setting** page will be configuration of the required ports as 'MAC Based' authentication (opposite to 'Port Based' authentication)


Save
Tools
Stack ID
1
Up Time:2 days 5:10:13
Logged in as administrator, admin - 192.168.0.100
Logout
DGS-3100-48
Configuration
L2 Features
QoS
Security
Safeguard Engine
Trusted Host
Port Security
Guest VLAN
802.1X
802.1X Setting
Authentic RADIUS
Forwarding EAP
SSL
SSH
Access Authentication
Monitoring
ACL
STACKING STATUS
802.1X Setting
Safeguard
802.1X
Enabled
Disabled
Apply
802.1X Port Access Control
QuietPeriod (0-65535) 60 sec
SuppTimeout (1-65535) 30 sec
ServerTimeout (1-65535) 30 sec
MaxReq (1-10) 2 times
TxPeriod (1-65535) 30 sec
ReAuthPeriod (300 - 4294967295) 3600 sec
ReAuthEnabled Enabled
Control ForceAuthorized
Unit 01
From Port 02
To Port 02
Mode MAC Base
Apply
List
Unit | Port | Control | TxPeriod | Quiet Period | Supp-Timeout | Server-Timeout | MaxReq | ReAuth Period | ReAuth Enabled | Mode
1 | 1:1 | Auto | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | PortBase
1 | 1:2 | ForceAuthorized | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | MAC Base
1 | 1:3 | ForceUnauthorized | 30 | 60 | 30 | 30 | 2 | 3600 | Enabled | PortBase
1 | 1:4 | Auto | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | PortBase
1 | 1:5 | Auto | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | PortBase
1 | 1:6 | Auto | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | PortBase
1 | 1:7 | Auto | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | PortBase
1 | 1:8 | Auto | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | PortBase

6. The last step on **Security > 802.1X > 802.1X Setting page** should be setting the port control to 'Auto', this will complete the setting of MAC Authentication for the required ports**.**


Save
Tools
Stack ID
1
Up Time:2 days 5:10:13
Logged in as administrator, admin - 192.168.0.100
Logout
DGS-3100-48
Configuration
L2 Features
QoS
Security
Safeguard Engine
Trusted Host
Port Security
Guest VLAN
802.1X
802.1X Setting
Authentic RADIUS
Forwarding EAP
SSL
SSH
Access Authentication
Monitoring
ACL
STACKING STATUS
802.1X Setting
Safeguard
802.1X
Enabled
Disabled
Apply
802.1X Port Access Control
QuietPeriod (0-65535) 60 sec
SuppTimeout (1-65535) 30 sec
ServerTimeout (1-65535) 30 sec
MaxReq (1-10) 2 times
TxPeriod (1-65535) 30 sec
ReAuthPeriod (300 - 4294967295) 3600 sec
ReAuthEnabled Enabled
Control Auto
Unit 01
From Port 02
To Port 02
Mode MAC Base
Apply
List
Unit | Port | Control | TxPeriod | Quiet Period | Supp-Timeout | Server-Timeout | MaxReq | ReAuth Period | ReAuth Enabled | Mode
1 | 1:1 | Auto | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | PortBase
1 | 1:2 | ForceAuthorized | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | MAC Base
1 | 1:3 | ForceUnauthorized | 30 | 60 | 30 | 30 | 2 | 3600 | Enabled | PortBase
1 | 1:4 | Auto | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | PortBase
1 | 1:5 | Auto | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | PortBase
1 | 1:6 | Auto | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | PortBase
1 | 1:7 | Auto | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | PortBase
1 | 1:8 | Auto | 30 | 60 | 30 | 30 | 2 | 3600 | Disabled | PortBase

Defining RADIUS Settings

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for management access.

The default parameters are user-defined, and are applied to newly defined RADIUS servers. If new default parameters are not defined, the system default values are applied to newly defined RADIUS servers.

1. Click **Security > 802.1X > Authentic RADIUS Server**. The *Authentic RADIUS Server Page* opens:

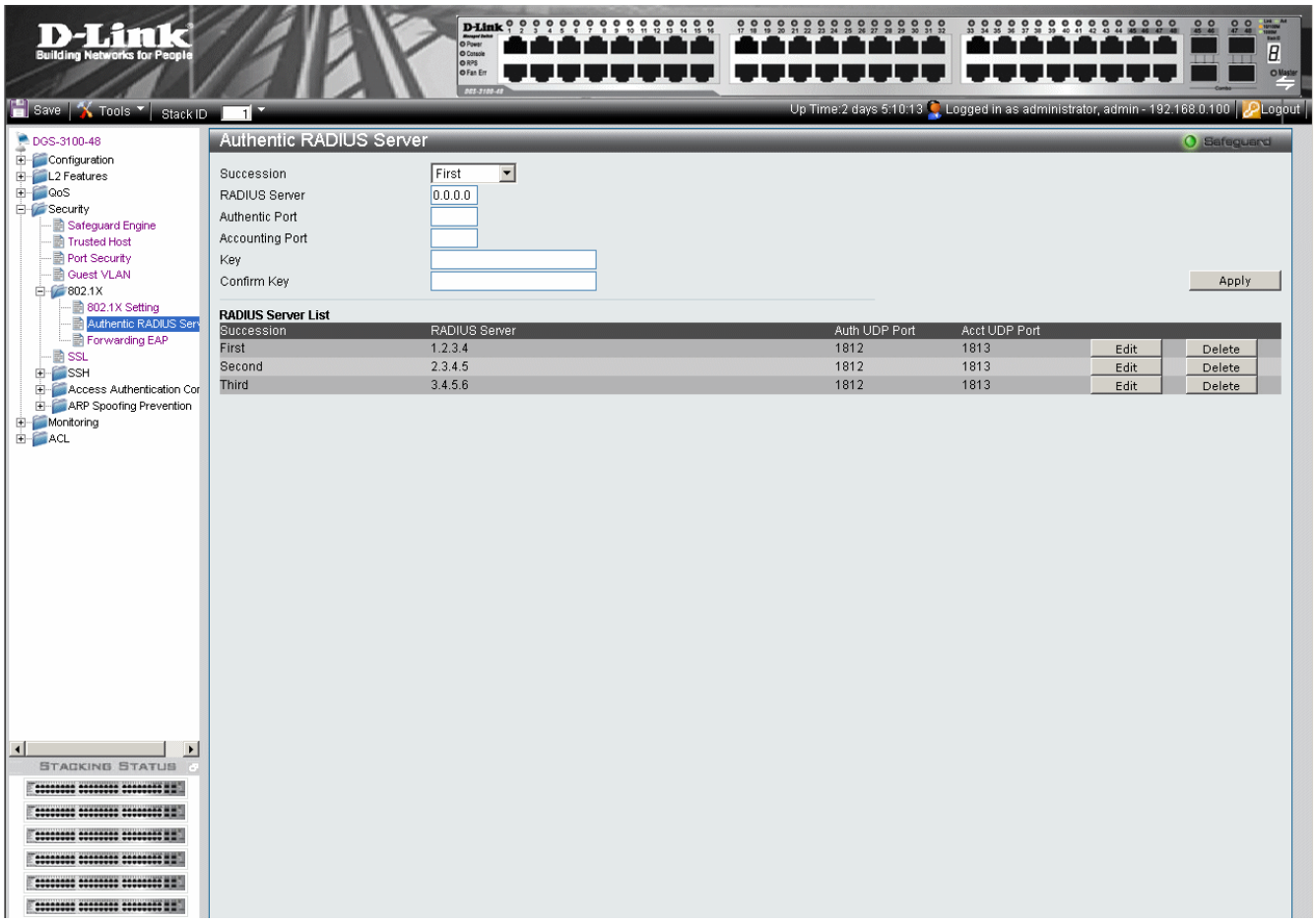


Figure 5-6 Authentic RADIUS Server Page

The Authentic RADIUS Server Page contains the following fields:

Field	Description
Succession	Defines the desired RADIUS server to configure. Network managers use up to 3 RADIUS servers for port authentication. The possible field values are: *First* — Indicates the RADIUS parameters are defined for the first RADIUS server. *Second* — Indicates the RADIUS parameters are defined for the second RADIUS server. *Third* — Indicates the RADIUS parameters are defined for the third RADIUS server.
RADIUS Server	Defines the RADIUS server IP addresses. The field format is X.X.X.X.
Authentic Port	Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.
Accounting Port	Defines the port used to send *Start* and *Stop* authentication messages. Information received through the RADIUS Accounting Port is recorded in the *RADIUS Authentication Page*. The default port is 1813.
Key	Defines the authentication and encryption key for communications between the device and the

Field	Description
	server. This key must match the encryption used on the server.
Confirm Key	Confirms the RADIUS key defined in the **Key** field.

2. Define the RADIUS server to configure in the Succession field.
3. Define the RADIUS server IP address in the RADIUS Server field.
4. Define the authentication port in the *Authentic Port* field.
5. Define the accounting port in the *Accounting Port* field.
6. Define the authentication and encryption key in the *Key* field.
7. Reenter the RADIUS Key in the *Confirm Key* field.
8. Click Apply.

- To edit the Radius Server list, click Edit adjacent to the required listed server. The upper fields display the current values, which then can be edited.
- To delete a radius server from the list, click Delete adjacent to the relative list entry. The radius servers are defined, and the device is updated.

Defining EAP Forwarding Settings

Ports use the *Extensible Authentication Protocol* (EAP) forwarding mechanism when 802.1x authentication is disabled. The *Forwarding EAP Page* allows the user to enable or disable forwarding EAP packets to an authentication server.

1. Click **Security > 802.1X > Forwarding EAP**. The *Forwarding EAP Page* opens:

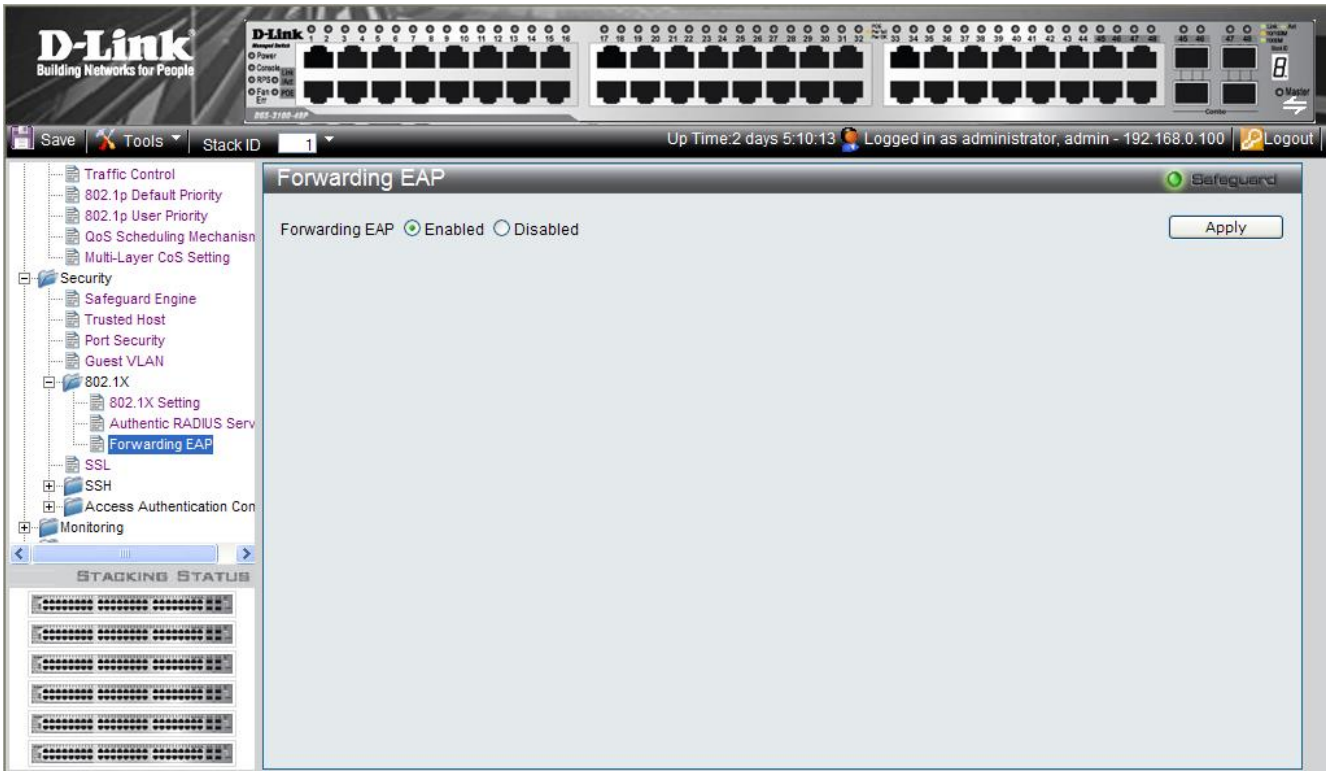


Figure 0-7 Forwarding EAP Page

The Forwarding EAP Page contains the following field:

Field	Description
Forwarding EAP	Specifies whether forwarding of EAP packets is enabled on the device. The possible field values are: *Enabled* — Enables forwarding of EAP packets. *Disabled* — Disables forwarding of EAP packets. This is the default.

2. Define the EAP packet forwarding status in the *Forwarding EAP* field.
3. Click Apply. The EAP packet forwarding status is defined, and the device is updated

Configuring Secure Socket Layer Security

Secure Socket Layer (SSL) is a security feature that provides a secure communication path between a host and client through the use of authentication, digital signatures, and encryption. These security functions are implemented using a *Ciphersuite*, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes used for authentication sessions, and that consists of:

- **Key Exchange** —Cyphersuite strings specify the public key algorithm used. This switch utilizes the *Rivest Shamir Adleman* (RSA) public key algorithm. This is the first authentication process between client and host as they "exchange keys" in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
- **Encryption:** The second part of the ciphersuite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:
  - *Stream Ciphers* – There are two types of stream ciphers on the Switch, *RC4 with 40-bit keys* and *RC4 with 128-bit keys*. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
  - *CBC Block Ciphers – Cipher Block Chaining* (CBC) links encrypted text blocks. The Switch supports the *3DES EDE* encryption code defined by the *Data Encryption Standard* (DES) to create the encrypted text.
- **Hash Algorithm** — This part of the ciphersuite allows the user to choose a message digest function which will determine a Message Authentication Code. This *Message Authentication Code* will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, *Message Digest 5* (*MD5*) and *Secure Hash Algorithm* (*SHA*).

The *SSL Configuration Settings Page* permits network managers to enable SSL with all supported ciphersuites on the Switch. Ciphersuites are security strings that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The Switch possesses three possible ciphersuites for the SSL function, which are enabled by default.

NOTE: Once SSL is enabled, the Web and Telnet are disabled.

To manage the device via an Embedded Web System while SSL is enabled, the web browser must support SSL encryption. URL headers must begin with *https://*, for example *https://10.90.90.90*.

The system supports up-to five SSH sessions.

To enable SSL on the device:

1. Click **Security > SSL**. The *SSL Configuration Settings Page* opens**:**

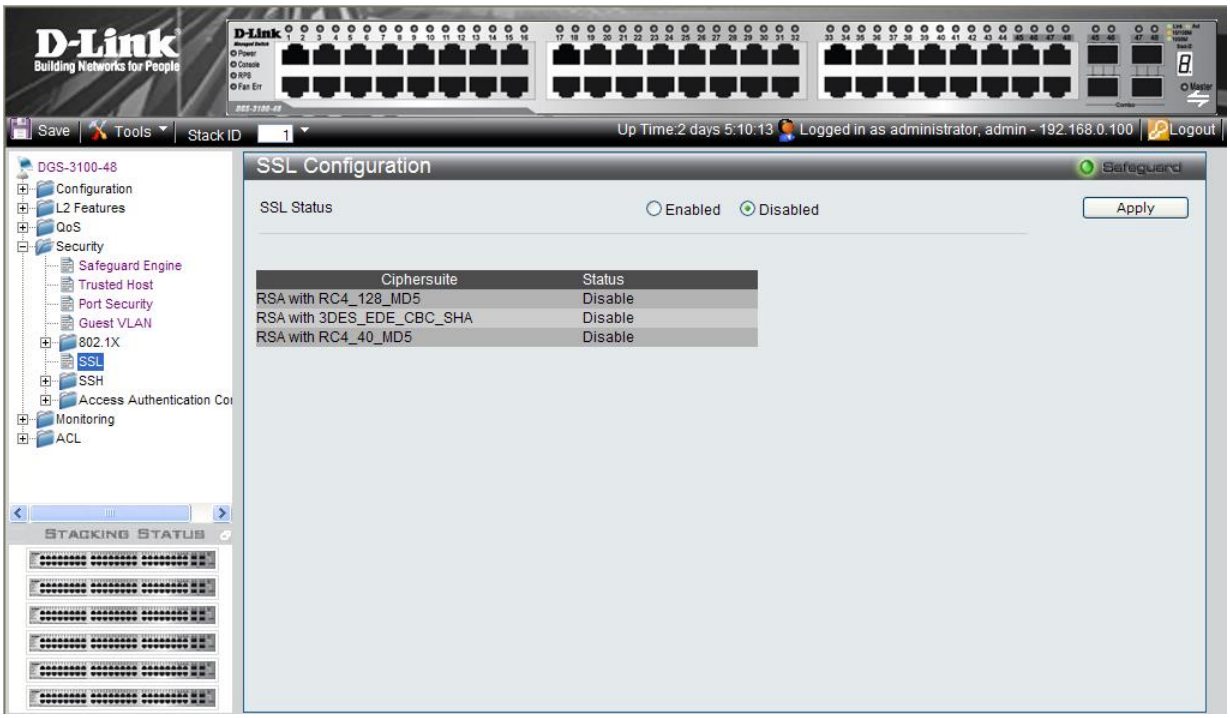


Figure 5-8 SSL Configuration Settings Page

The SSL Configuration Settings Page contains the following fields:

Field	Description
SSL Status	Indicates if SSL is enable on the device. The possible field values are: *Enabled* — Indicates SSL is enabled on the device. *Disabled* — Indicates SSL is disabled on the device. (This is the default value.)
Ciphersuite	Indicates the Ciphersuite. The possible field values are: *RSA with RC4 128 MD5* —Combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. *RSA with 3DES EDE CBC SHA* — This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. *RSA EXPORT with RC4 40 MD5* — This ciphersuite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys.
Status	Indicates if the selected Ciphersuite is enable or disabled for SSL. The possible field values are: *Enable* — Enables the Ciphersuite for SSL. *Disable* — Disables the Ciphersuite for SSL.

2. Enable or disable the SSL status in the ***SSL Status*** field.
3. Click Apply. The SSL status is defined, and the device is updated.

Configuring Secure Shell Security

Secure Shell permits network users to securely login to the network from a remote location over an insecure network. SSH a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

Ensure the following steps are completed before configuring SSH:

- Create a user account with admin-level access using the **User Accounts** window in the **Administration folder**. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.
- Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the **Current Accounts** window (**Security** > **Secure Shell (SSH)** > **SSH User Authentication**). There is a special SSH method that mey be used to authorize the user: *Public Key*. The default value is *None*.

NOTE: DGS-3100-xx only supports SSH protocol version 2.

To define SSH on the device:

1. Click **Security > SSH > SSH** Configuration. The *SSH Configuration Page* opens:

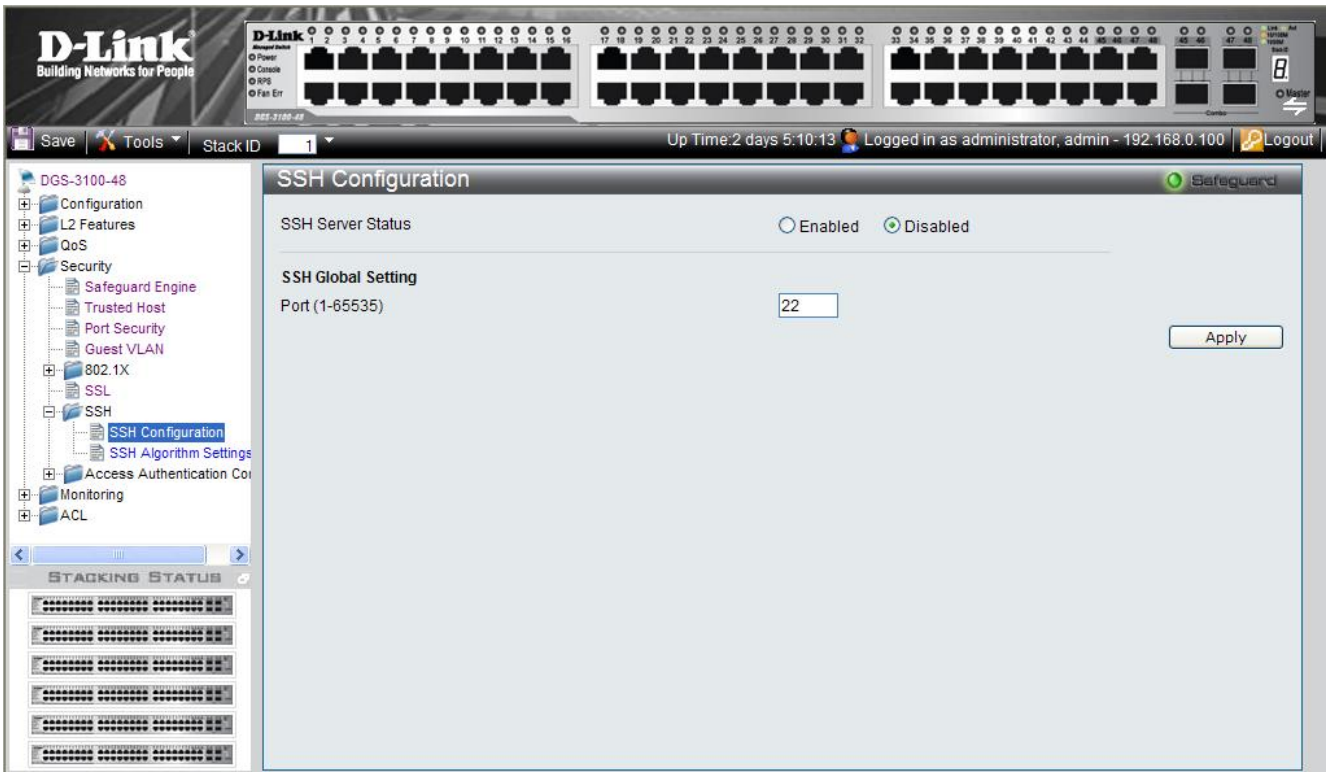


Figure 5-9. SSH Configuration Page

The SSH Configuration Page contains the following fields:

Field	Description
SSH Server Status	Indicates if SSH is enabled on the device. The possible field values are:

Field	Description
	Enable — Enables SSH on the device. *Disable* — Disables SSH on the device. This is the default value.
Port (1-65535)	Displays the port number used to authenticate the SSH session. The possible field range is 1-65535. The field default is 22.

2. Enable or disable the SSH server status in the *SSH Server Status* field.
3. Define the SSH global setting port number in the *Port (1-65535)* field.
4. Click Apply. The SSH configuration is defined, and the device is updated.

Defining SSH Algorithm Settings

This *SSH Algorithm Settings Page* allows network administrators to enable a public key for SSH authentication encryption. The following authentication keys are enabled for SSH:

- **Public Key Algorithm** — Encrypt a cryptographic key pair composed of a public key and a private key. The private key is kept secret, while the public key can be distributed. The encryption keys are mathematically similar, but a private key cannot be derived from the public key. Messages encrypted with a public key can be decrypted with the matching private key. The following Public Key Algorithms are supported:
  - *HMAC-RSA* — Supports the *Hash for Message Authentication Code* (HMAC) mechanism utilizing the RSA encryption algorithm.
  - HMAC-DSA —Supports the Hash for Message Authentication Code (HMAC) Digital Signature Algorithm (DSA) encryption algorithm.
- **Data Integrity Algorithm** — Validates message authentication information transmitted between two parties which share the same key. The following Data Integrity Algorithms are supported:
  - *HMAC-SHA* — Supports the Hash for Message Authentication Code (HMAC) Secure Hash Algorithm (SHA) mechanism.
  - *HMAC MD5* — Supports the Hash for Message Authentication Code (HMAC) MD5 Message Digest (MD5) mechanism.
- **Encryption Algorithm** — Generates authentication keys used to authenticate communications between different applications. The following Encryption Algorithms are supported
  - *3DES-CBC* — Support a block size of 8 bytes (64 bits); its key size is 192 bits long. The first 8 bytes cannot be identical to the second 8 bytes, and the second 8 bytes cannot be identical to the third 8 bytes.
  - *AES128* —Provide a block cipher that encrypts and decrypts digital information. The AES128 algorithm is capable of using cryptographic 128 keys.
  - *AES192* — Provides a block cipher that encrypts and decrypts digital information. The AES192 algorithm is capable of using cryptographic 192 keys.
  - *AES256* — Provide a block cipher that encrypts and decrypts digital information. The AES256 algorithm is capable of using cryptographic 256 keys.
  - *RC4* — Supports a cipher with an up to 2048 bits key size.

All algorithms are enabled by default. To enable SSH Algorithms:

1. Click **Security > SSH > SSH Algorithm Settings**. The *SSH Algorithm Settings Page* opens**:**

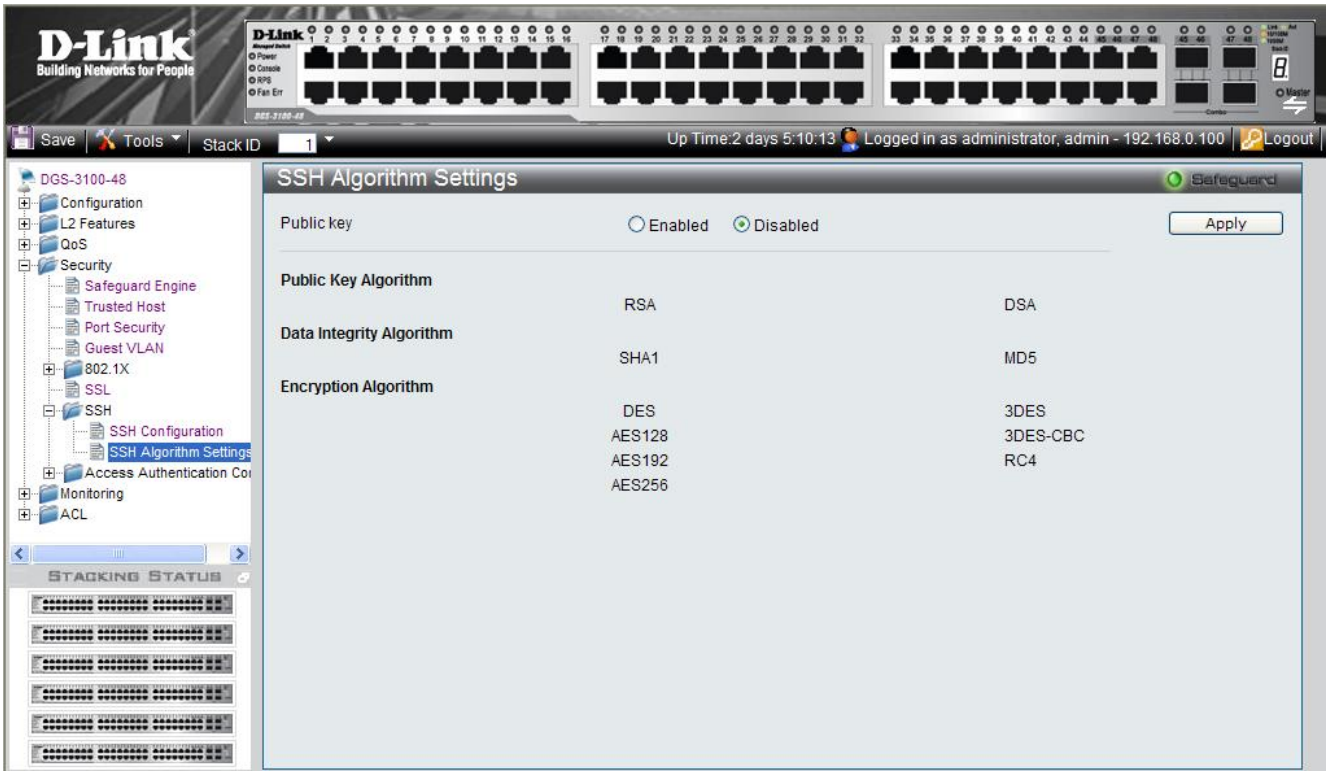


Figure 5-10 SSH Algorithm Settings Page

The SSH Algorithm Settings Page contains the following fields:

Field	Description
Public key	Indicates Publickey SSH User Authentication enabled on the device. The possible field values are: *Enabled* — Enables Publickey SSH User Authentication on the device. *Disable* — Disables Publickey SSH User Authentication on the device. Disable is the default value.
Public Key Algorithm	Displays the currently enabled Public Key Algorithms.
Data Integrity Algorithm	Displays the currently enabled Data Integrity Algorithms.
Encryption Algorithm	Displays the currently enabled Encryption Algorithms.

2. Enable or disable the public key status in the *Public key* field.
3. Click Apply. The Publickey SSH User Authentication setting is defined, and the device is updated.

Defining Application Authentication Settings

Application Authentication permits network administrators to assign authentication methods for user authentication. For example, console users can be authenticated by Authentication List 1, while Telnet users are authenticated by Authentication List 2.

1. Click **Security > Access Authentication Control > Application Authentication Settings**. The *Application Authentication Settings Page* opens**:**

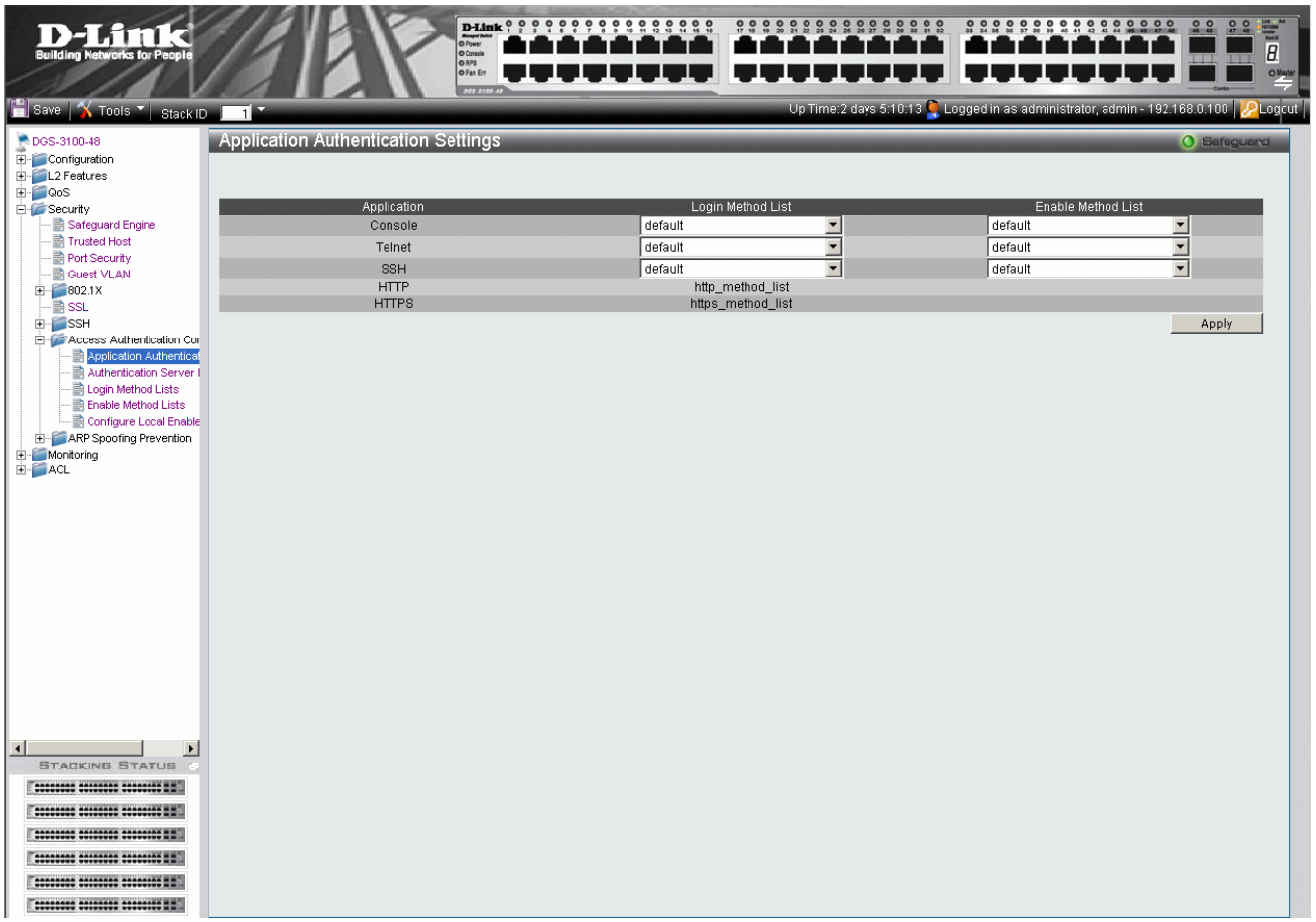


Figure 5-11 Application Authentication Settings Page

The Application Authentication Settings Page contains the following fields:

Field	Description
Application	Indicates the authentication application for which the Login Method or Enable Method lists are defined. The possible field values are: *Console* — Indicates that Authentication profiles are used to authenticate console users. *Telnet* — Indicates that Authentication profiles are used to authenticate Telnet users. *Secure Telnet (SSH)* — Indicates that Authentication profiles are used to authenticate Secure Shell (SSH) users. SSH provides clients secure and encrypted remote connections to a device.
Login Method List	Defines the method used by the application to authenticate normal login. http_method_list and https_method_list are fixed method names for http and https respectively.
Enable Method List	Defines the method used by the application to enable a normal login.

2. **S**elect the login method for the Console, Telnet, and Secure Telnet (SSH) from the list under *Login Method List*.
3. Select the enable method for the Console, Telnet, and Secure Telnet (SSH) from the list under *Enable Method List*.

4. Click Apply. The Application Authentication settings are defined, and the device is updated**.**

Configuring Authentication Server Hosts

The Authentication Server is a remote device connected to the same network as the Client and Authenticator. Users are authenticated using either RADIUS or TACACS+, and must be authenticated by the server before attaining network access. To define the Authentication Server information:

1. Click **Security > Access Authentication Control> Authentication Server Hos**t. The *Authentication Server Host Page* opens:

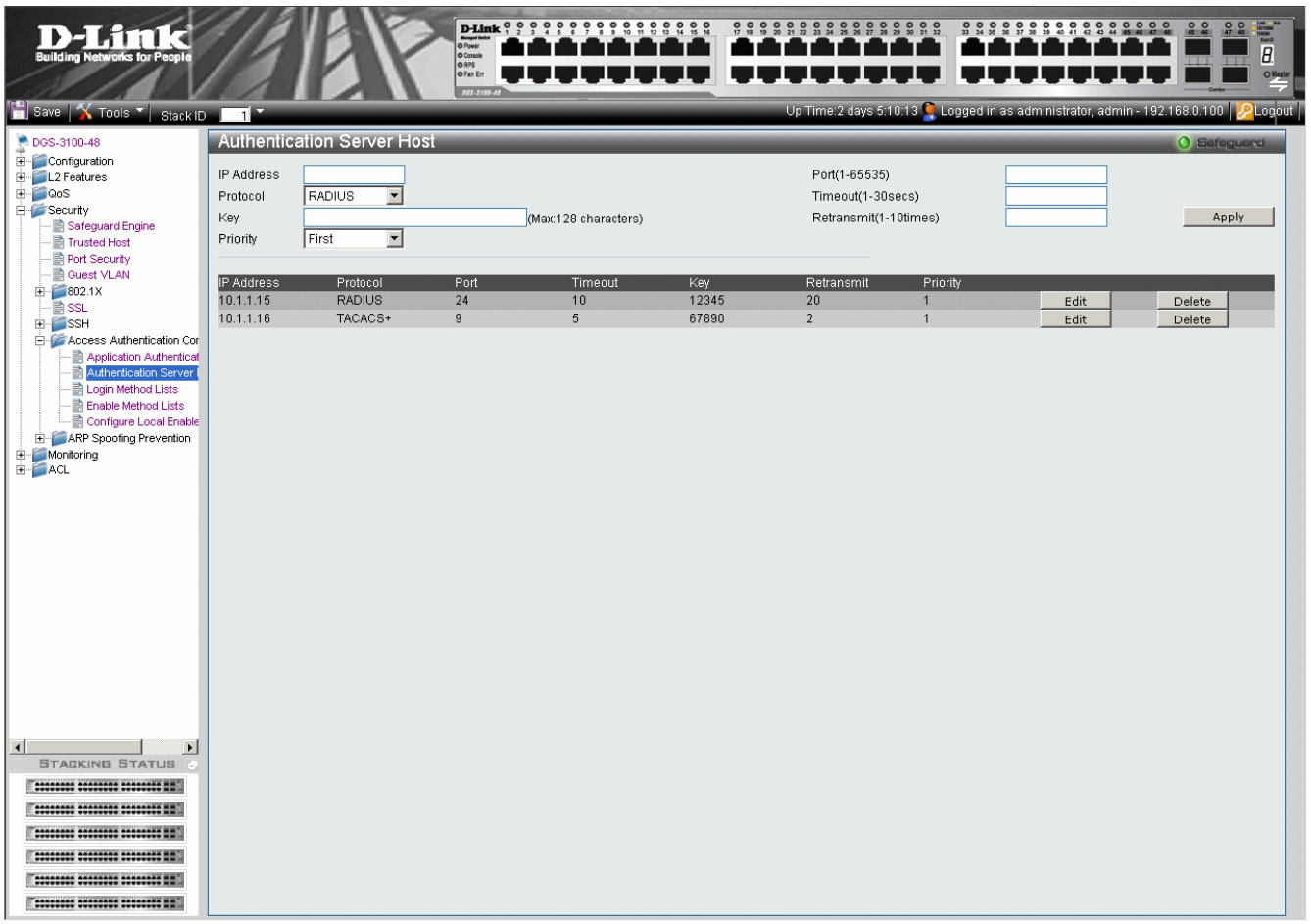


Figure 5-12 Authentication Server Host Page

The Authentication Server Host Page contains the following fields:

Field	Description
IP Address	Defines the IP address of the RADIUS or TACACS+ server authenticating network users.
Protocol	Indicates the authentication protocol used to authenticate network users. The possible field values are: *RADIUS* — Indicates that network users are authenticated via a RADIUS server. *TACACS+* — Indicates that network users are authenticated via a TACACS+ server.
Key	Defines the key used to authenticate network users. The key may contain up to 128 characters
Priority	Defines the priority assigned to the server. The field range is First -Third, where Third is the lowest priority and First is the highest priority.
Port (1-65535)	The port number for authentication requests. The host is not used for authentication if set to 0. If unspecified, the Radius port number defaults to 1812, TACACS+ port number defaults to 49.

Field	Description
Timeout (1-30secs)	Indicates the amount of time that passes, in which no authentication activity occurs, after which the authentication session times out.
Retransmit (1-10 times)	Indicates the number of times the port attempts to re- authenticate a timed out session.

2. Define the IP Address, Protocol, Key, Port, Timeout, and Retransmit fields**.**
3. Click Apply.The Authentication Host properties are defined, and the device is updated.

- To edit an authentication, click Edit adjacent to the relevant IP Address on the list. The upper fields display the current values, which then can be edited.
- To delete an authentication, click Delete adjacent to the relevant IP Address on the list. The Authentication Server settings are defined, and the device is updated.

Defining Login Methods

Network users must first login to the device on the *Login Method Lists* Page. Access as non-administrative users is granted. To configure the device as a Network Administrator, the user must also log on to the device on the *Enable Method Lists Page*.

User authentication occurs in the order the methods are selected. If the first authentication method is not available, the next selected method is used. For example, if the selected authentication method is RADIUS, Local, and the RADIUS server is not available, the user is authenticated locally. To define the user only login method:

1. Click **Security > Access Authentication Control > Login Method Lists.** The *Login Method Lists Page* opens:

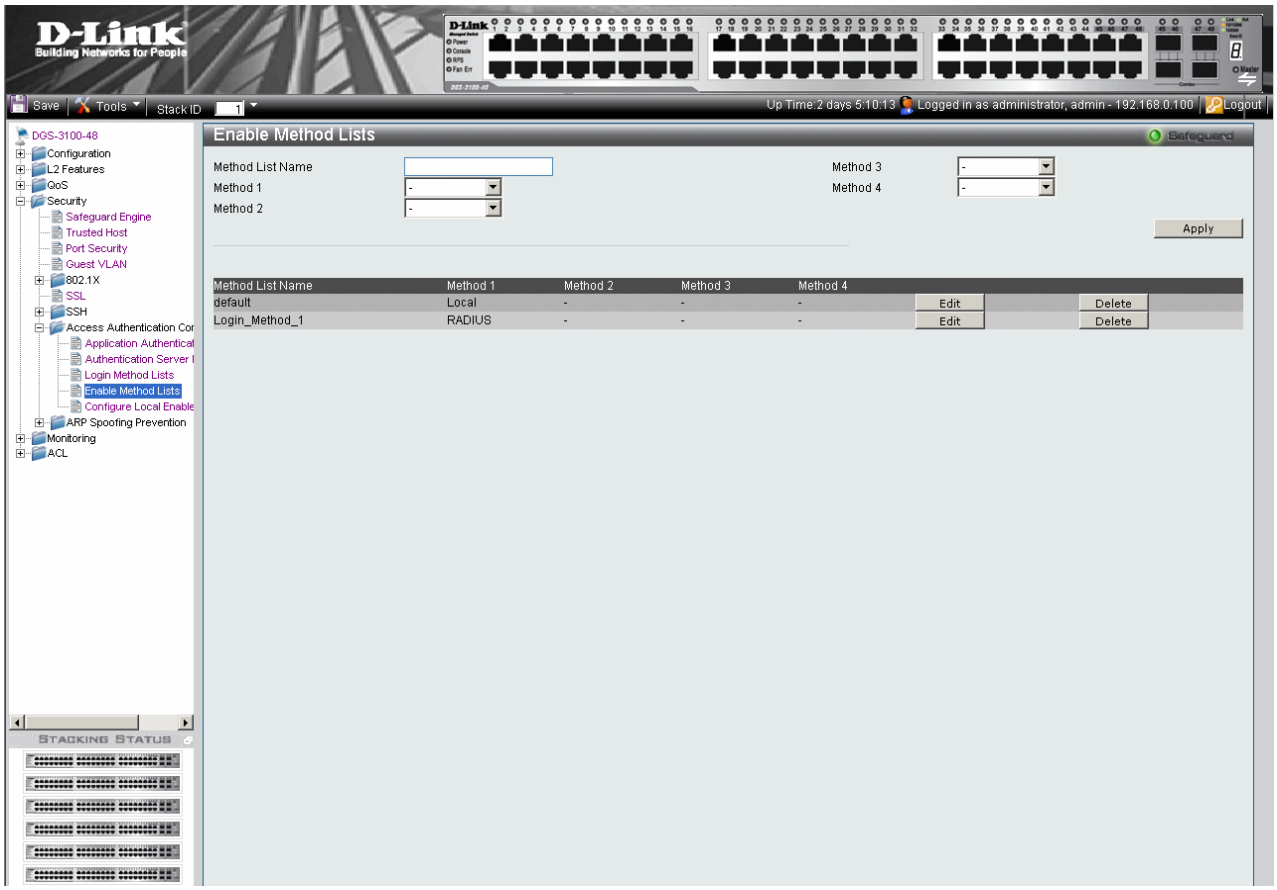


Figure 5-13 Login Method Lists Page

The Login Method Lists Page contains the following fields:

Field	Description

Field	Description
Method List Name	Displays the method list name. The field is user-defined besides the http_method_list and https_method_list which cannot be deleted or renamed.
Method 1	Indicates the first method used to authenticate the network user. The possible field values are: *RADIUS* — User authentication occurs at the RADIUS server. *TACACS+* — The user authentication occurs at the TACACS+ server. *None* — No user authentication occurs. *Local* — User authentication occurs at the device level. The device checks the user name and password for authentication.
Method 2	Indicates the second method used to authenticate the network user. The possible field values are: *RADIUS* — User authentication occurs at the RADIUS server. *TACACS+* — The user authentication occurs at the TACACS+ server. *None* — No user authentication occurs. *Local* — User authentication occurs at the device level. The device checks the user name and password for authentication.
Method 3	Indicates the third method used to authenticate the network user. The possible field values are: *RADIUS* — User authentication occurs at the RADIUS server. *TACACS+* — The user authentication occurs at the TACACS+ server. *None* — No user authentication occurs. *Local* — User authentication occurs at the device level. The device checks the user name and password for authentication.
Method 4	Indicates the fourth method used to authenticate the network user. The possible field values are: *RADIUS* — User authentication occurs at the RADIUS server. *TACACS+* — The user authentication occurs at the TACACS+ server. *None* — No user authentication occurs. *Local* — User authentication occurs at the device level. The device checks the user name and password for authentication.

2. Define the Method List Name in the *Method List Name* field.
3. Select the methods used to authenticate network users in the *Method 1, Method 2, Method 3 and, Method 4* fields.
4. Click Apply. The Login methods are defined, and the device is updated.

- To edit the Method List, click Edit adjacent to a Method List Name on the list. The upper fields display the current values, which then can be edited.
- To delete a Method List Name, click Delete. The Login Method Lists are defined, and the device is updated.

Defining Enable Methods

Network users must first login to the device on the *Enable Method Lists* Page. Access as non-administrative users is granted.

The *Enable Method Lists* Page allows network mangers to assign user privileges using authentication methods on the device. Once a user is assigned a normal user level privileges the network user is authenticated and granted network access and configuration privileges. A maximum of four Enable Method Lists can be defined on the device. The Enable Method List cannot be deleted but can be configured.

User authentication occurs in the order the methods are selected. If the first authentication method is not available, the next selected method is used. For example, if the selected authentication method is RADIUS, Local, and the RADIUS server is not available; the user is authenticated locally. To define authentication methods:

1. Click **Security > Access Authentication Control > Enable Method Lists**. The *Enable Method Lists Page* opens:

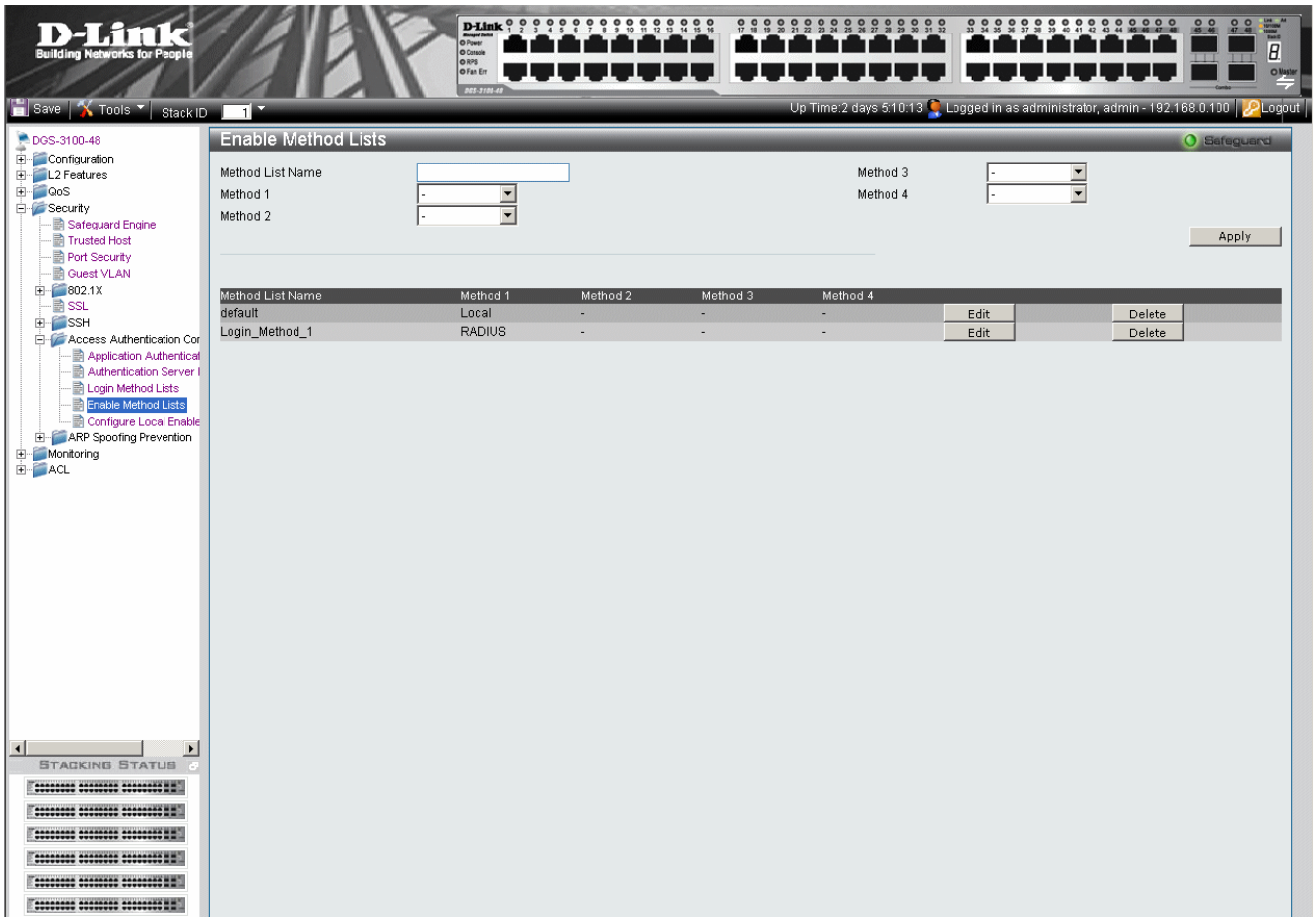


Figure 5-14 Enable Method Lists Page

The Enable Method Lists Page contains the following fields:

Field	Description
Method List Name	Defines the method list name. The field is user-defined besides the http_method_list and https_method_list which cannot be deleted or renamed.
Method 1	Indicates the first method used to authenticate the network user. The possible field values are: *RADIUS* — User authentication occurs at the RADIUS server. *TACACS+* — The user authentication occurs at the TACACS+ server. *None* — No user authentication occurs. *Local* — User authentication occurs at the device level. The device checks the user name and password for authentication.

Field	Description
Method 2	Indicates the second method used to authenticate the network user. The possible field values are: *RADIUS* — User authentication occurs at the RADIUS server. *TACACS+* — The user authentication occurs at the TACACS+ server. *None* — No user authentication occurs. *Local* — User authentication occurs at the device level. The device checks the user name and password for authentication.
Method 3	Indicates the third method used to authenticate the network user. The possible field values are: *RADIUS* — User authentication occurs at the RADIUS server. *TACACS+* — The user authentication occurs at the TACACS+ server. *None* — No user authentication occurs. *Local* — User authentication occurs at the device level. The device checks the user name and password for authentication.
Method 4	Indicates the fourth method used to authenticate the network user. The possible field values are: *RADIUS* — User authentication occurs at the RADIUS server. *TACACS+* — The user authentication occurs at the TACACS+ server. *None* — No user authentication occurs. *Local* — User authentication occurs at the device level. The device checks the user name and password for authentication.

2. Define the Method List Name in the *Method List Name* field.
3. Select the methods used to authenticate network users in the *Method 1, Method 2, Method 3 and, Method 4* fields.
4. Click Apply. The Enable method and passwords are defined, and the device is updated.

- To edit the Enable Method List, click Edit adjacent to an Enable Method List Name on the list. The upper fields display the current values, which then can be edited.
- To delete an Enable Method List Name, click Delete. The Enable Method Lists are defined, and the device is updated.

Configuring Local Enable Password

The *Configure Local Enable Password Page* allows network administrators to configure the local enabled password. To define the network Local Enable password:

1. Click **Security > Access Authentication Control > Configure Local Enable Password**. The *Configure Local Enable Password Page* opens**:**

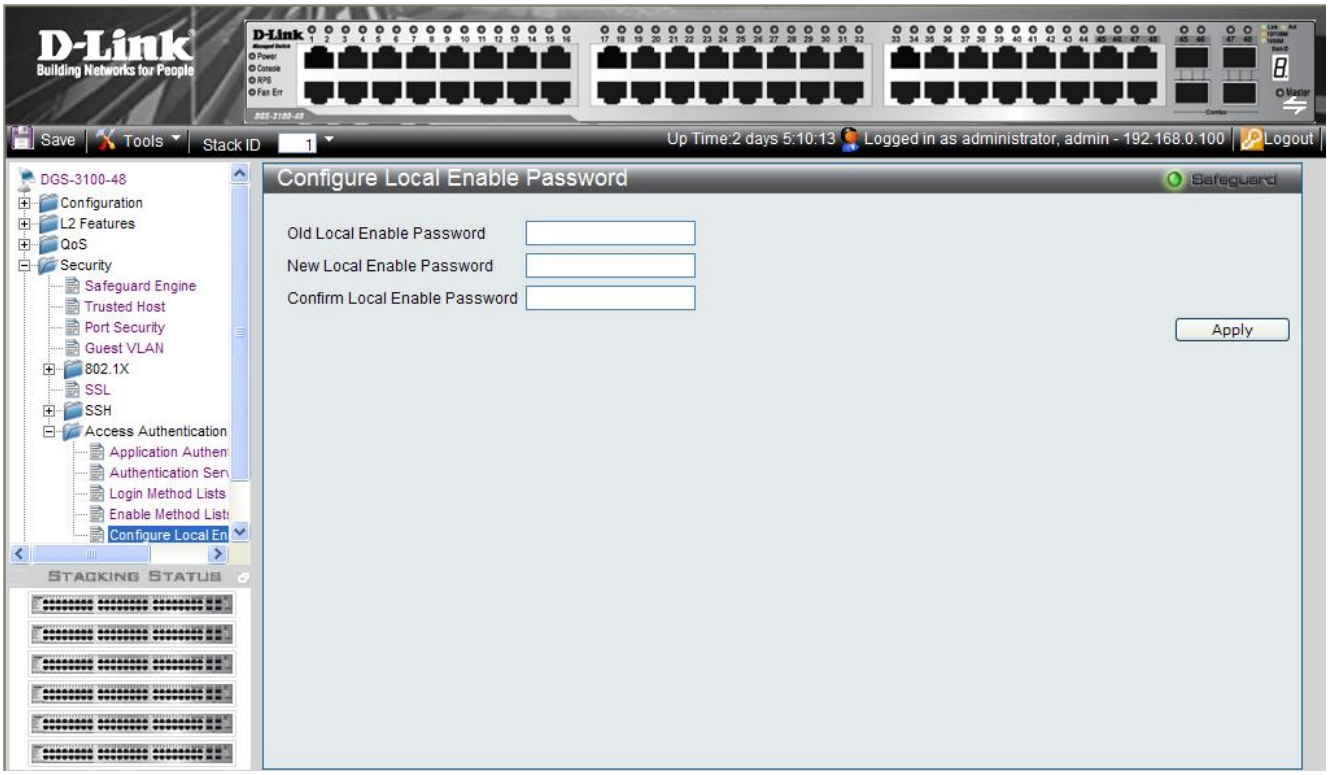


Figure 5-15 Configure Local Enable Password Page

The Configure Local Enable Password Page contains the following fields:

Field	Description
Old Local Enable Password	Provide the current network Enable password.
New Local Enable Password	Defines the new network Enable password. The field range is 1-15 characters.
Confirm Local Enable Password	Confirms the new network Enable password.

2. Enter the old local enable password In the *Old Local Enable Password* field.
3. Define the new local enable password in the *New Local Enable Password* field.
4. Re-enter the new password in the *Confirm Local Enable Password* field.
5. The new local enable password is configured, and the device is updated.

Defining ARP Spoofing Prevention Settings

Classic *Address Resolution Protocol* (ARP) is a TCP/IP protocol that translates IP addresses into MAC addresses.

ARP Spoofing Prevention eliminates man-in-the-middle attacks, where false ARP packets are inserted into the subnet. ARP requests and responses are inspected, and their MAC Address to IP Address binding is checked. Packets with invalid ARP Spoofing Prevention Bindings are logged and dropped. If the incoming packet's source IP address is not one of the gateways defined in the ARP Spoofing prevention database, the packet is forwarded.

The Arp Spoofing Prevention Page provides parameters for enabling and setting global ARP Spoofing Prevention parameters, as well as defining ARP Spoofing Prevention Log parameters. Up to 240 entries can be defined.

To define ARP Spoofing Prevention:

1. Click **Security > Arp Spoofing Prevention**. The *Arp Spoofing Prevention Page* opens:

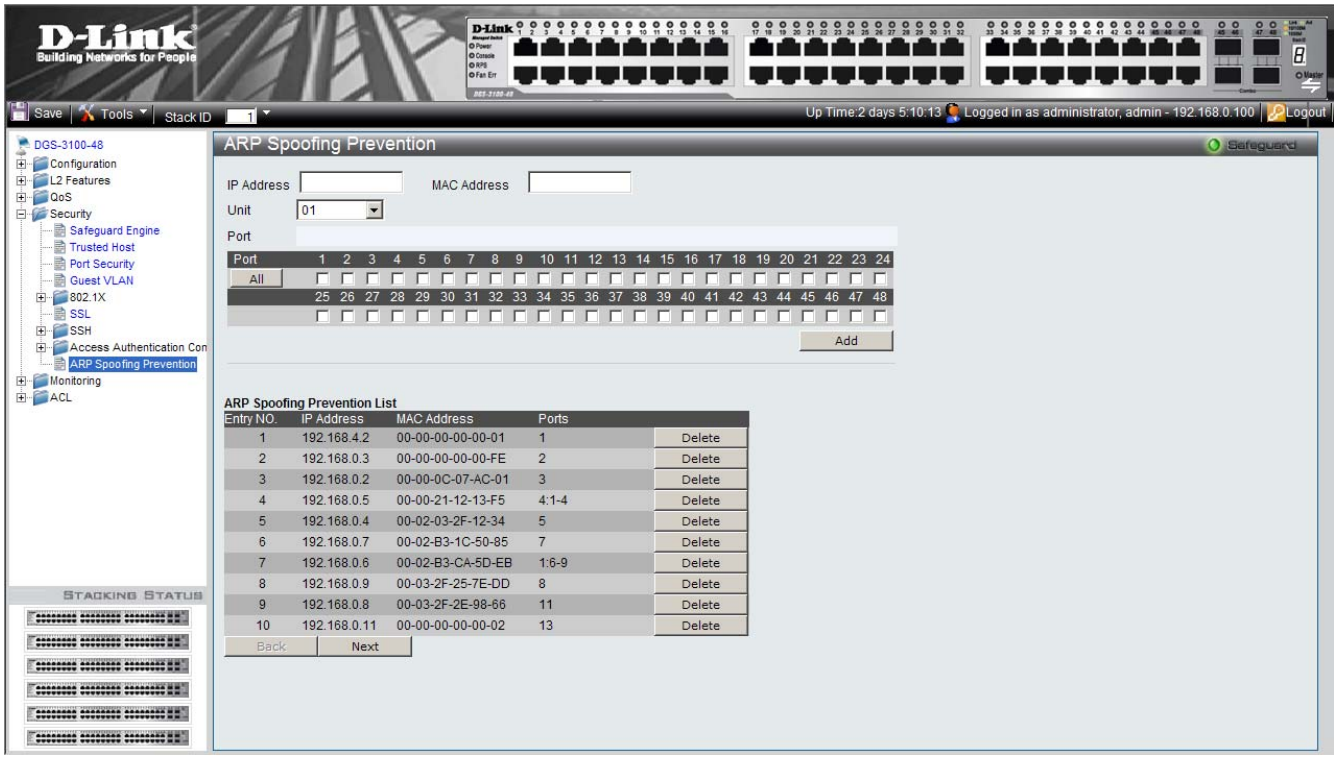


Figure 5-16 Arp Spoofing Prevention Page

The Arp Spoofing Prevention Page contains the following fields

Field	Description
IP Address	Specifies IP addresses included in ARP Binding Lists that are checked against ARP requests.
MAC address	Specifies MAC addresses included in ARP Binding Lists that are checked against ARP requests.
Unit	Displays the stacking member for which the ARP Spoofing Prevention is displayed.
Port	Defines the Port Settings Mode. The possible field values are: • *Checked Ports* — Indicates that a packet received on the port needs to be checked for a match with the ARP Spoofing Prevention database. • *Unchecked Ports* — Indicates that the port is not selected for ARP Spoofing (trusted port). ARP packets that are received on unchecked interfaces are forwarded.
Port	Specifies IP addresses included in ARP Binding Lists that are checked against

Field	Description
	ARP requests.

2. Click Apply. The device is updated with the ARP Spoofing Prevention configuration.

6

MONITORING THE DEVICE

This section contains information for view device and packet statistics as well as, viewing IGMP information and MAC address information. This section includes the following topics:

- Device Environment
- Errors
- Cable Diagnostics
- Viewing Stacking Information
- Viewing CPU Utilization
- Viewing Port Utilization
- Viewing Packet Size Information
- Viewing Received Packet Statistics
- Viewing RADIUS Authenticated Session Statistics
- Viewing ARP Table
- Viewing MLD Router Ports
- Viewing Router Ports
- Viewing Session Table
- Viewing IGMP Group Information
- Viewing MLD Group Information
- Defining Dynamic and Static MAC Addresses
- Viewing System Log
- Green Ethernet
- Device Environment
- Errors
- Cable Diagnostics

Viewing Stacking Information

The *Stacking Information Page* provides specific information for stacked devices. To show the Stacking Information Page:

1. Click Tools, and from the menu select *Show Stack Status.*
2. Alternatively, click **Monitoring > Stacking Information** in the Tree View. The *Stacking Information Page* opens:

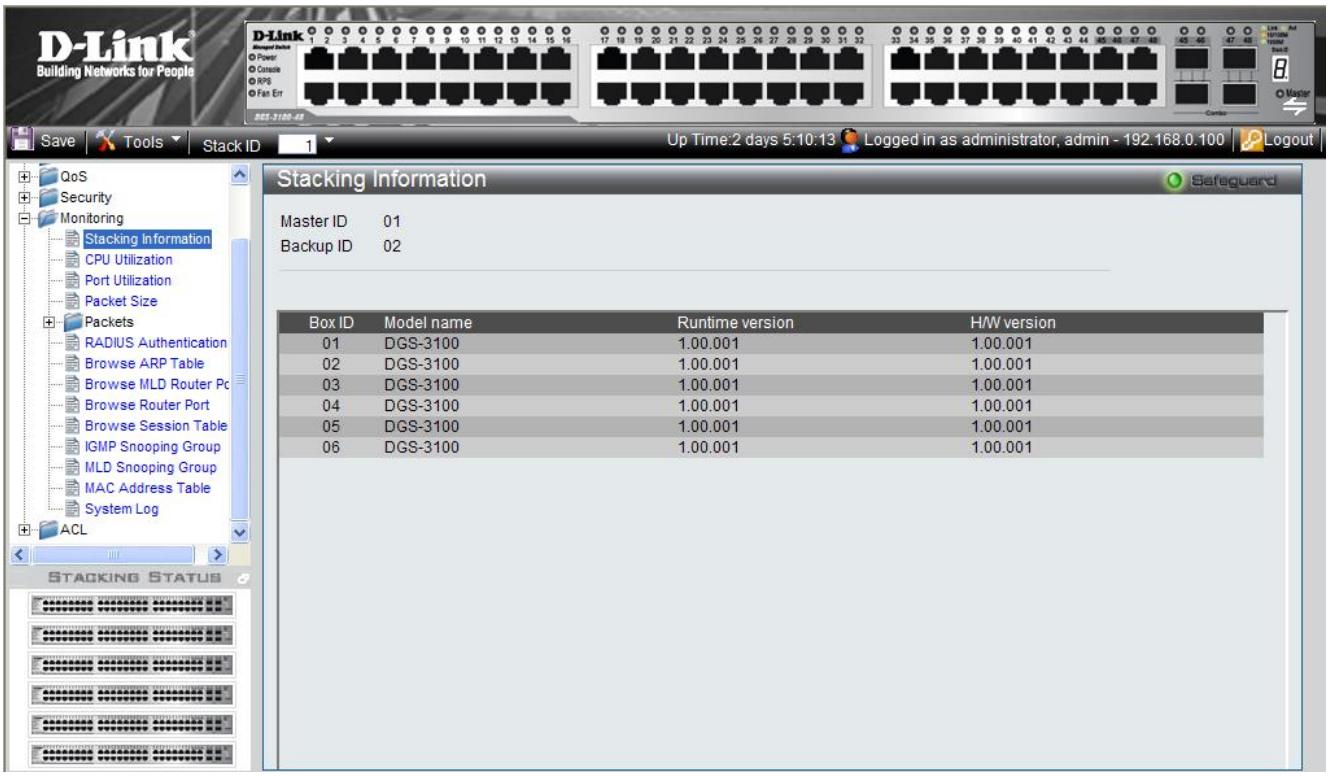


Figure 6-1 Stacking Information Page

The Stacking Information Page contains the following fields:

Field	Description
Master ID	Displays the Stacking Master Unit ID number. (unit ID 1 or 2).
Backup ID	Displays the Backup Master Unit ID number. (unit ID 1 or 2).
Box ID	Displays the Unit ID numbers assigned to the stacking members.
Runtime version	Indicates the software version running on the device.
H/W version	Displays the stacking member's hardware version.

Viewing CPU Utilization

The *CPU Utilization Page* contains information about the system's CPU utilization.

1. Click **Monitoring > CPU Utilization**. The *CPU Utilization Page* opens:

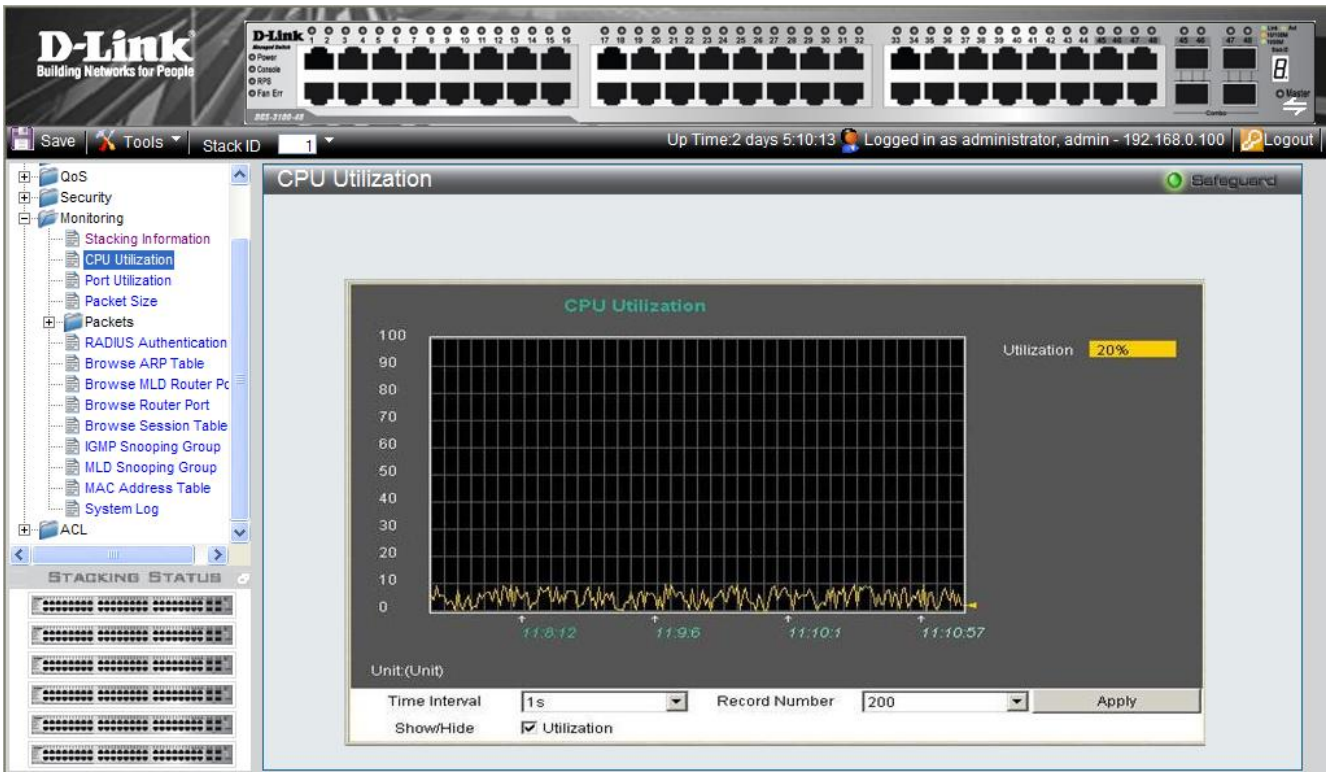


Figure 6-2 CPU Utilization Page

The CPU Utilization Page contains the following fields:

Field	Description
Utilization	Displays current CPU utilization by percentage.
Time Interval	Defines the 1-60 second time intervals in which the usage samples are taken as follows: 1,2,3,4,5,10,20,30,40,50,60.
Record Number	Defines the record number.
Show/Hide	Displays the CPU utilization information. The possible fields are: *Utilization checked* — Utilization information is enabled. This is the default value. *Utilization unchecked* — Utilization information is disabled.

2. Define the Time Interval and Record Number fields.
3. Define the *Show/Hide* field.
4. Click Apply. A sample record of CPU utilization is stored, and the device is updated.

Viewing Port Utilization

The *Port Utilization Page* contains port utilization information for specific ports. To view port statistics:

1. Click **Monitoring > Port Utilization**. The *Port Utilization Page* opens:

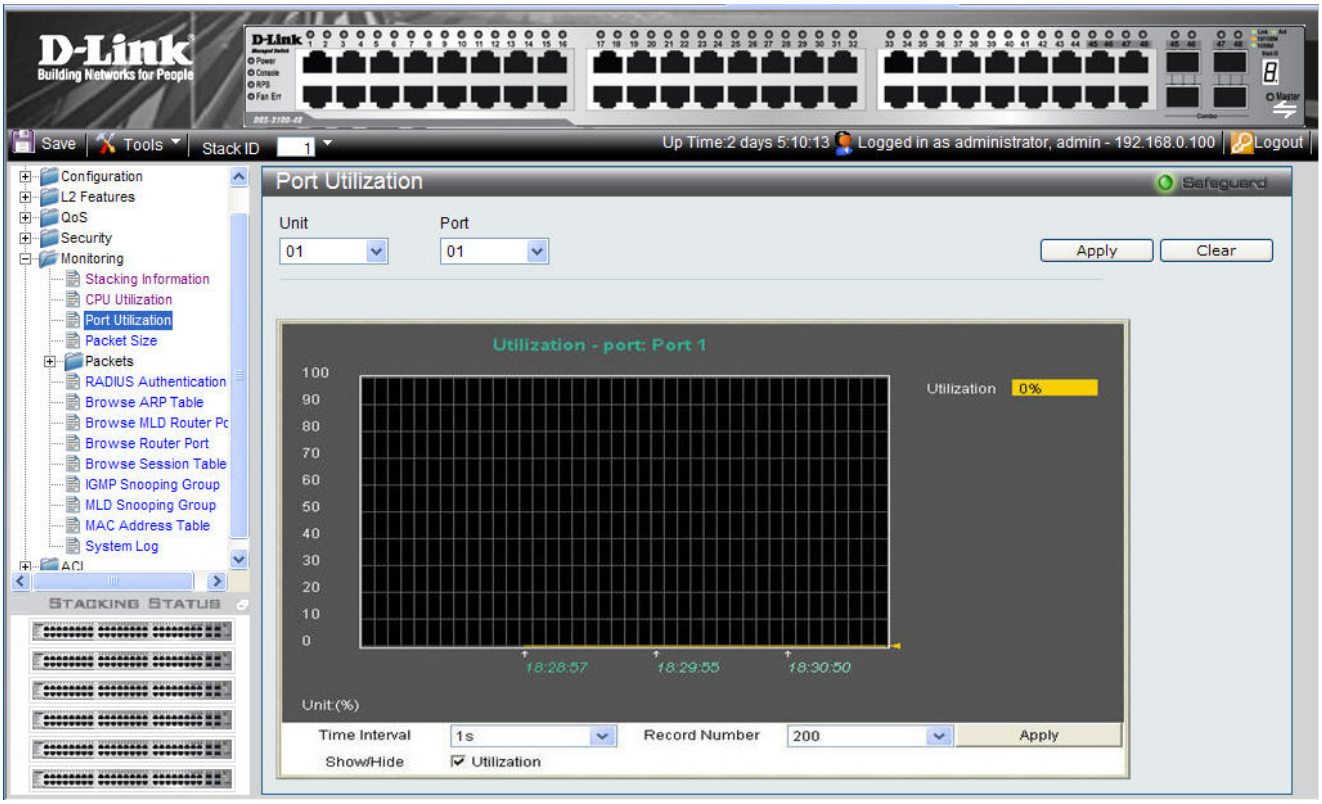


Figure 0-3 Port Utilization Page

The Port Utilization Page contains the following fields:

Field	Description
Unit	Defines the unit number.
Port	Defines the port number.
Utilization	Displays current CPU utilization by percentage.
Time Interval	Defines the 1-60 second time intervals in which the usage samples are taken as follows: 1,2,3,4,5,10,20,30,40,50,60.
Record Number	Defines the record number.
Show/Hide	Displays the CPU utilization information. The possible fields are: *Utilization checked* — Utilization information is enabled .This is the default value. *Utilization unchecked* — Utilization information is disabled.

2. Define the Unit, Port, Time Interval, and Record Number fields.
3. Define the *Show/Hide* field**.**
4. Click Apply. A sample record of CPU port utilization is stored, and the device is updated.

Viewing Packet Size Information

The *Packet Size Page* displays packets received by the switch, arranged in seven groups and classed by size, to be viewed as either a line graph or a table.

1. Click **Monitoring > Packet Size**. The *Packet Size Page* opens:

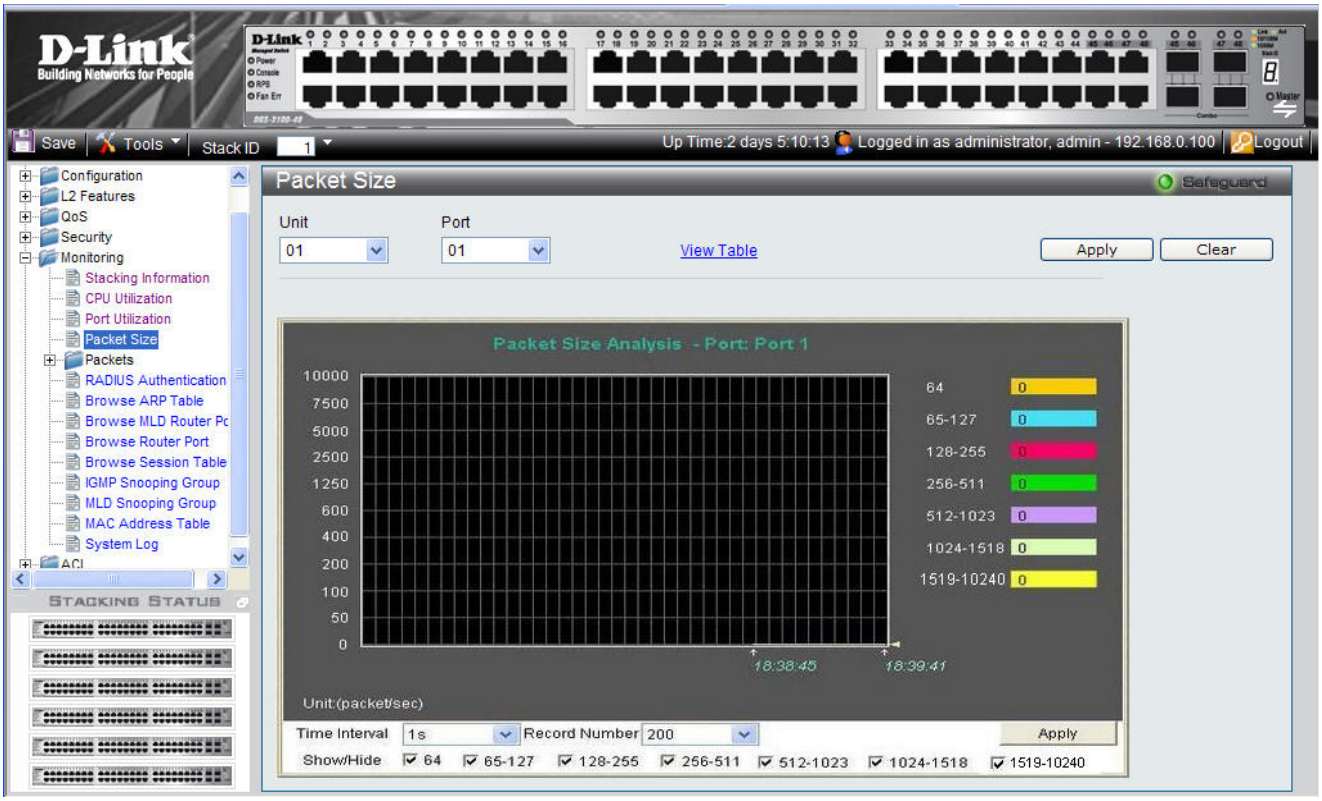


Figure 6-4 Packet Size Page

The Packet Size Page contains the following fields:

Field	Description
Unit	Defines the unit number.
Port	Defines the port number.
Packet Size Analysis – Selected Port Number	Displays current packet size for ports.
Time Interval	Displays the time intervals at which the packet samples are taken. The possible field values are: 1s - 5s, 10s, 15s, 20s, 30s, 40s, 50s, and 60s.
Record Number	Displays the packet size record number.
Show/Hide	Displays or hides packets size. The following packet length ranges can be displayed: 64, 65-127, 128-255, 256-511, 512-1023 and, 1024-1518 and 1519-10240.

2. Click Apply. A sample record of packet size analysis is stored, and the device is updated.
3. Define the *Show/Hide* field.
4. To view the graph as a table, click View Table.

Viewing Received Packet Statistics

The *Received(RX) Page* contains information about packets transmitted through device ports. To view received packet statistics:

1. Click **Monitoring > Packets > Received(RX)**. The *Received(RX) Page* opens:

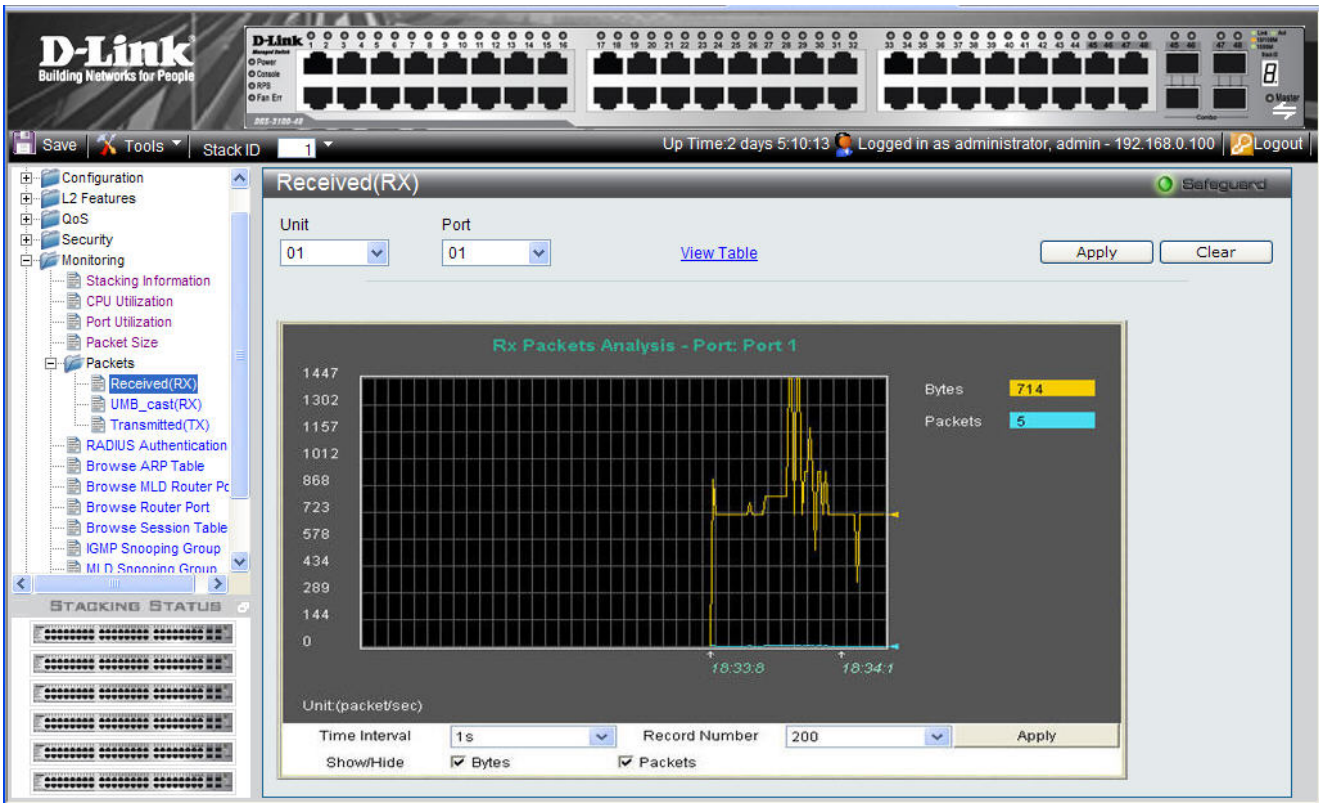


Figure 6-5 Received(RX) Page

The Received(RX) Page contains the following fields:

Field	Description
Unit	Displays the stacking member for which the transmitted packet statistics are displayed.
Port	Indicates the port for which the received packets parameters are displayed.
Bytes	Indicates the total number of bytes that were received on the port.
Packets	Indicates the total number of packets that were received on the port.
Time Interval	Indicates the time interval for which the received packets are displayed. The possible field values are: 1s - 5s, 10s, 15s, 20s, 30s, 40s, 50s, and 60s.
Record Number	Indicates the transmitted record number.
Show/Hide	Displays the bytes/packets received information. The possible fields are: *Bytes checked* — Checked displays the total amount of received bytes. *Packets checked* — Checked displays the total amount of received packets.

2. Define the *Unit* and *Port* fields.
3. Click Apply to load the defined parameters.
4. Define the Time Interval and Record Number fields.
5. Click Apply. The selected RX packet analysis is displayed.

6. Define the ***S**how/Hide* field.
7. To view the graph as a table, click View Table**.**

Viewing UMB_cast Packet Statistics

The *UMB_cast(RX) Page* displays the number of UMB cast (Unicast, Multicast and Broadcast) packets received on the device.

1. Click **Monitoring > Packets > UMB_cast(RX)**. The *UMB_cast(RX) Page* opens:

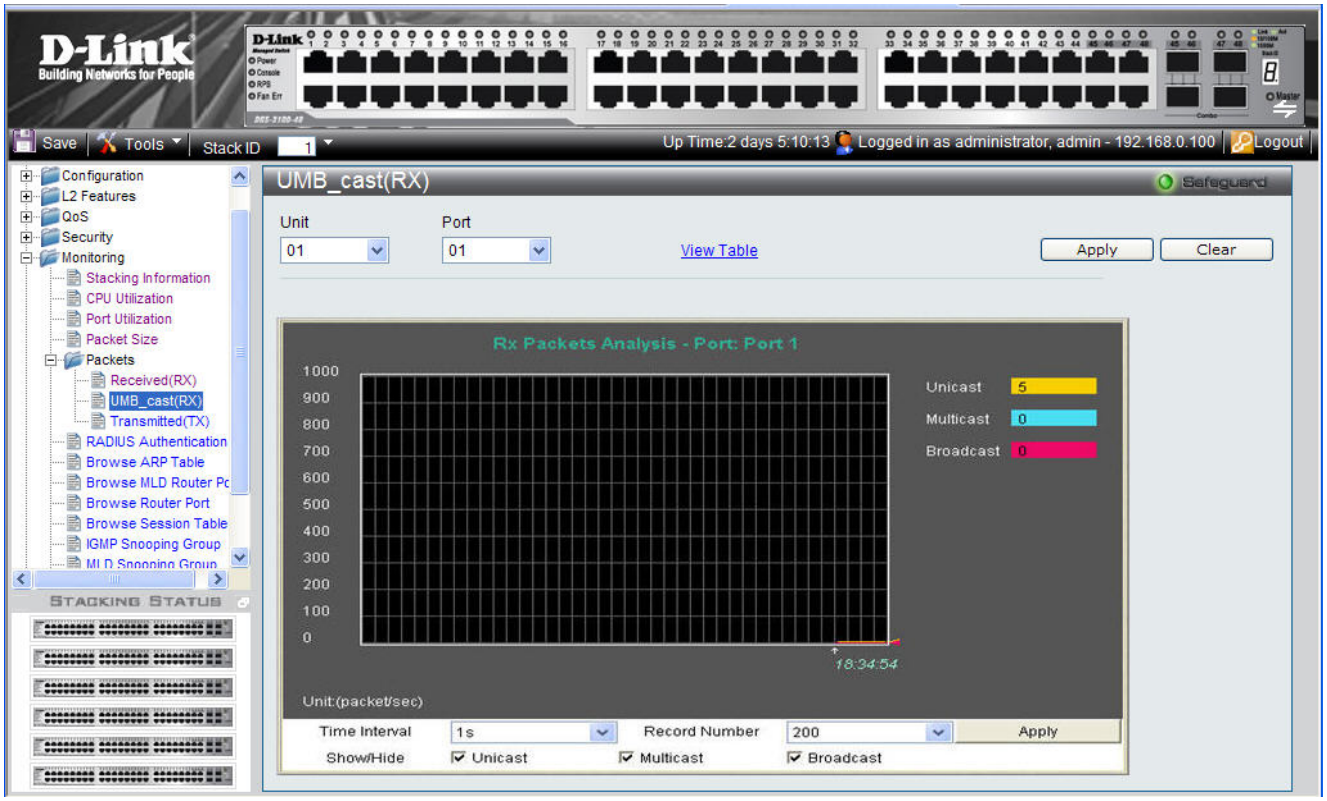


Figure 6-6 UMB_cast(RX) Page

The UMB_cast(RX) Page contains the following fields:

Field	Description
Unit	Indicates the stacking member for which the UMB_cast packets are displayed.
Port	Indicates the port for which the UMB_cast packets parameters are displayed.
Unicast	Indicates the number of Unicast packets received and transmitted through the device.
Multicast	Indicates the number of Multicast packets received and transmitted through the device.
Broadcast	Indicates the number of Broadcast packets received and transmitted through the device.
Time Interval	Indicates the time interval for which the UMB_cast packets are displayed. The possible field values are: 1s - 5s, 10s, 15s, 20s, 30s, 40s, 50s, and 60s.
Record Number	Indicates the transmitted record number.
Show/Hide	Displays the packets received information. The possible field values are: *Unicast checked* — Displays the total amount of transmitted Unicast packets. *Multicast checked* — Displays the total amount of transmitted Multicast packets. *Broadcast checked* — Displays the total amount of transmitted Broadcast packets.

2. Define the *Unit* and *Port* fields.
3. Click Apply to load the defined parameters.

To clear the *Unit* and *Port* fields:

1. Click Clear. The fields are cleared.
2. Define the Time Interval and Record Number fields.
3. Click Apply. The selected UMB_Cast (RX) packet analysis is displayed
4. To view the graph as a table, click View Table.

Viewing Transmitted Packet Statistics

The *Transmitted(TX) Page* contains information about packets transmitted through device ports. To view transmitted packet statistics:

1. Click **Monitoring > Packets >Transmitted(TX).** The *Transmitted(TX) Page* opens:

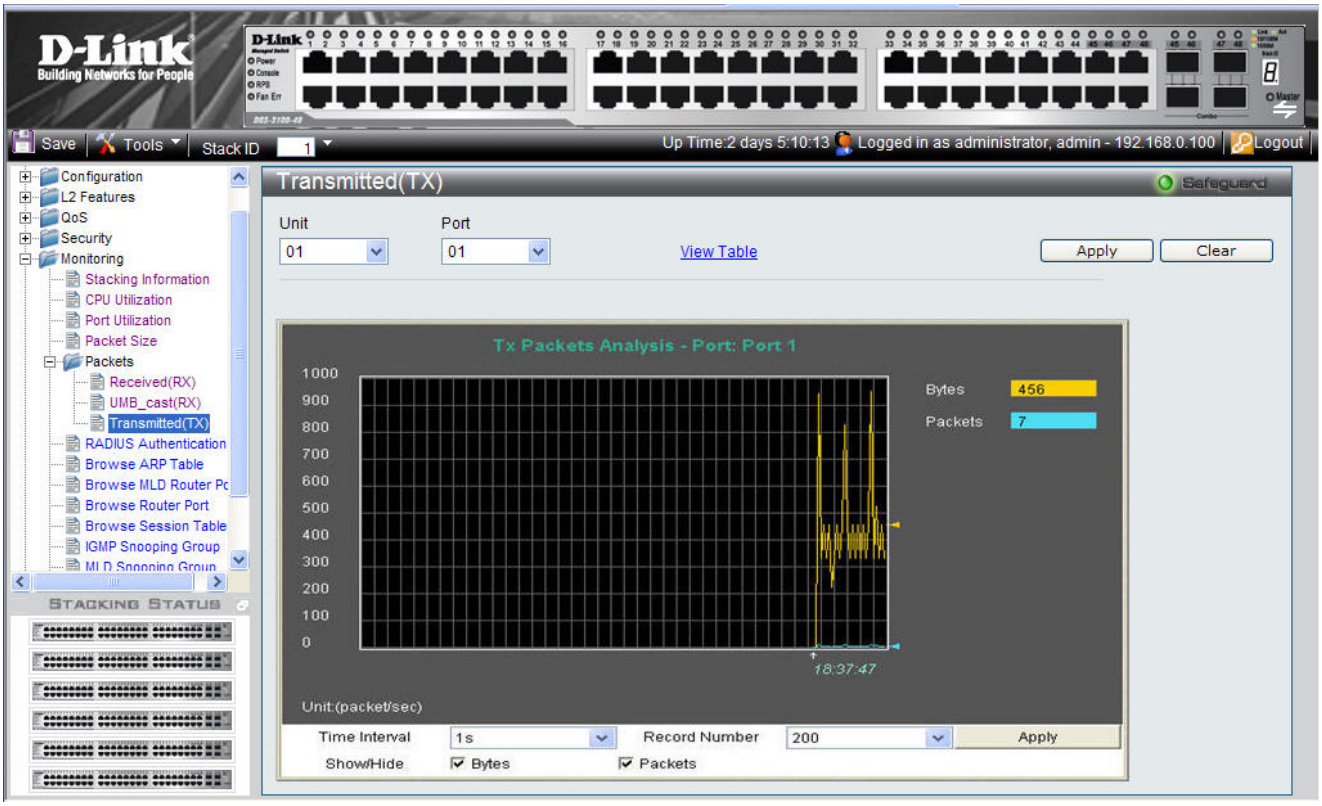


Figure 6-7 Transmitted(TX) Page

The Transmitted(TX) Page contains the following fields:

Field	Description
Unit	Indicates the stacking member ID for which the transmitted packets parameters are displayed.
Port	Indicates the port for which the transmitted packets parameters are displayed.
Bytes	Indicates the total number of bytes that were transmitted through the port.
Packets	Indicates the total number of packets that were transmitted through the port.
Time Interval	Indicates the time interval for which the transmitted packets are displayed. The possible field values are: 1s - 5s, 10s, 15s, 20s, 30s, 40s, 50s, and 60s.
Record Number	Indicates the transmitted record number.
Show/Hide	Displays the bytes/packets received information. The possible field values are: *Bytes checked* — Displays the total amount of transmitted bytes. *Packets checked* — Displays the total amount of transmitted packets.

2. Define the Unit and Port fields.
3. Click Apply to load the defined parameters.
4. To clear the *Unit* and *Port* fields:
5. Click Clear. The fields are cleared.
6. Define the Time Interval and Record Number fields.
7. Click Apply. The transmitted packet graph is updated.
8. To view the graph as a table, click View Table.

Viewing RADIUS Authenticated Session Statistics

The *RADIUS Authentication Page*provides RADIUS authentication sessions, including how many sessions were initiated, which ports intimated the authentication sessions, and whether or not the sessions were granted.

1. Click **Monitoring > Port Access Control > RADIUS Authentication**. The *RADIUS Authentication Page* opens:

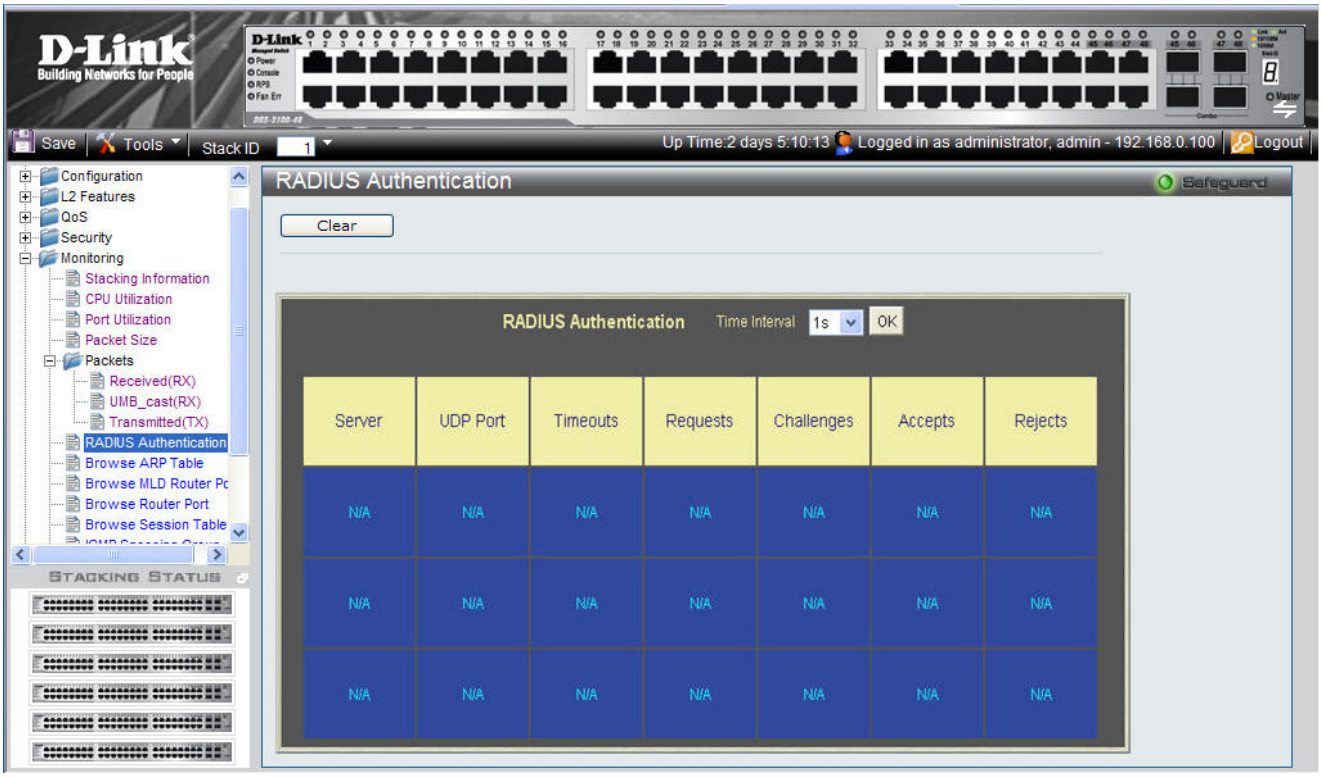


Figure 6-8 RADIUS Authentication Page

The RADIUS Authentication Pagecontains the following fields:

Field	Description
Time Interval	Indicates the how often the RADIUS authentication session information is updated. The various time intervals are: 15/30/60/no refresh.
Server	Displays the RADIUS server IP address.
UDP Port	Displays the UDP port through which the RADIUS session was initiated.
Timeouts	Indicates the number of session timeouts that occurred during the authentication session.
Requests	Indicates the amount of times the port requested an authentication session.
Challenges	Indicates the amount of times the port was challenged during an authentication session.
Accepts	Indicates the amount of authentication sessions initiated by the port which were accepted.
Rejects	Indicates the amount of authentication sessions initiated by the port which were rejected.

Viewing ARP Table

The *Browse ARP Table Page* provides information regarding ARP VLANs, including which IP address was mapped to what MAC address. To view the ARP table:

1. Click **Monitoring > Browse ARP Table**. The *Browse ARP Table Page* opens:

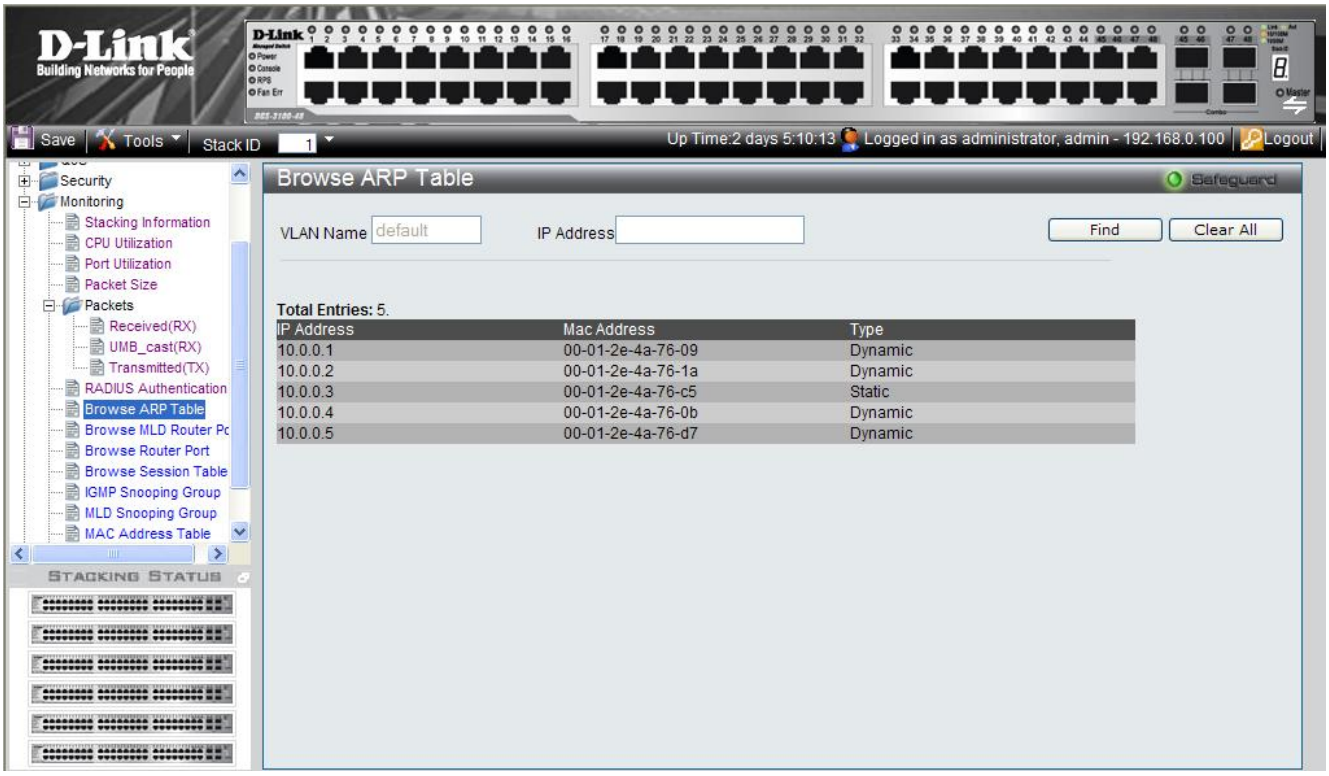


Figure 6-9 Browse ARP Table Page

The Browse ARP Table Page contains the following fields:

Field	Description
VLAN Name	Defines the VLAN for which the ARP mappings are defined.
IP Address	Defines the station IP address, which is associated with the MAC address.
Total Entries	Displays current ARP table entries, detailing the user defined interface name, IP address, MAC address and type (dynamic or static) of each entry.
MAC Address	Displays the MAC address associated with the IP address..
Type	Indicates how the MAC was assigned. The possible values are: – Dynamic — Indicates that the MAC address is dynamically created. – Static — Indicates the MAC address is a static IP address.

2. Click Find. The table updates and displays the values required.
3. Click Clear to clear the Browse ARP Table Page.

Viewing MLD Router Ports

The *Browse MLD Router Port Page* displays which ports are connected to MLD routers. A port can be connected to an MLD router either as a static port or as a dynamic port or forbidden port.

1. Click **Monitoring > Browse MLD Router Port**. The *Browse MLD Router Port Page* opens**:**

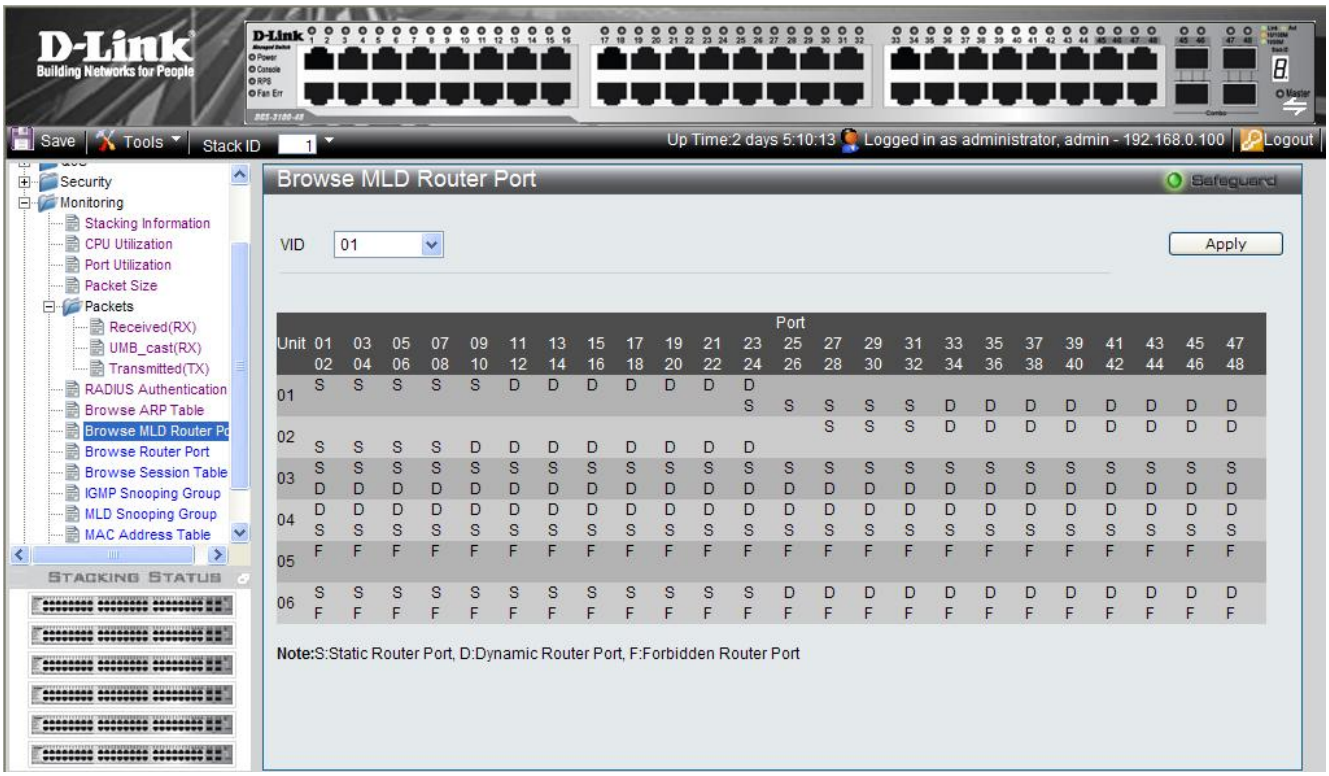


Figure 0-10 Browse MLD Router Port Page

The Browse MLD Router Port Page contains the following fields:

Field	Description
VID	Indicates the VLAN identification.
Unit	Indicates the stacking member for which the router ports information is displaying.
Port	Indicates the port for which the router port settings are displayed. Ports have the following settings: *S* — Indicates a statically configured port. *D* — Indicates a dynamically learned port. *F* — Indicates a forbidden port.

2. Define the *VID* field.
3. Click Apply. The selected ports appear on the selected VLAN**.**

Viewing Router Ports

The *Browse Router Port Page* displays which ports are connected to routers. Ports can be connected to routers either as a static port or as a dynamic port.

1. Click **Monitoring > Browse Router Port**. The *Browse Router Port Page* opens:

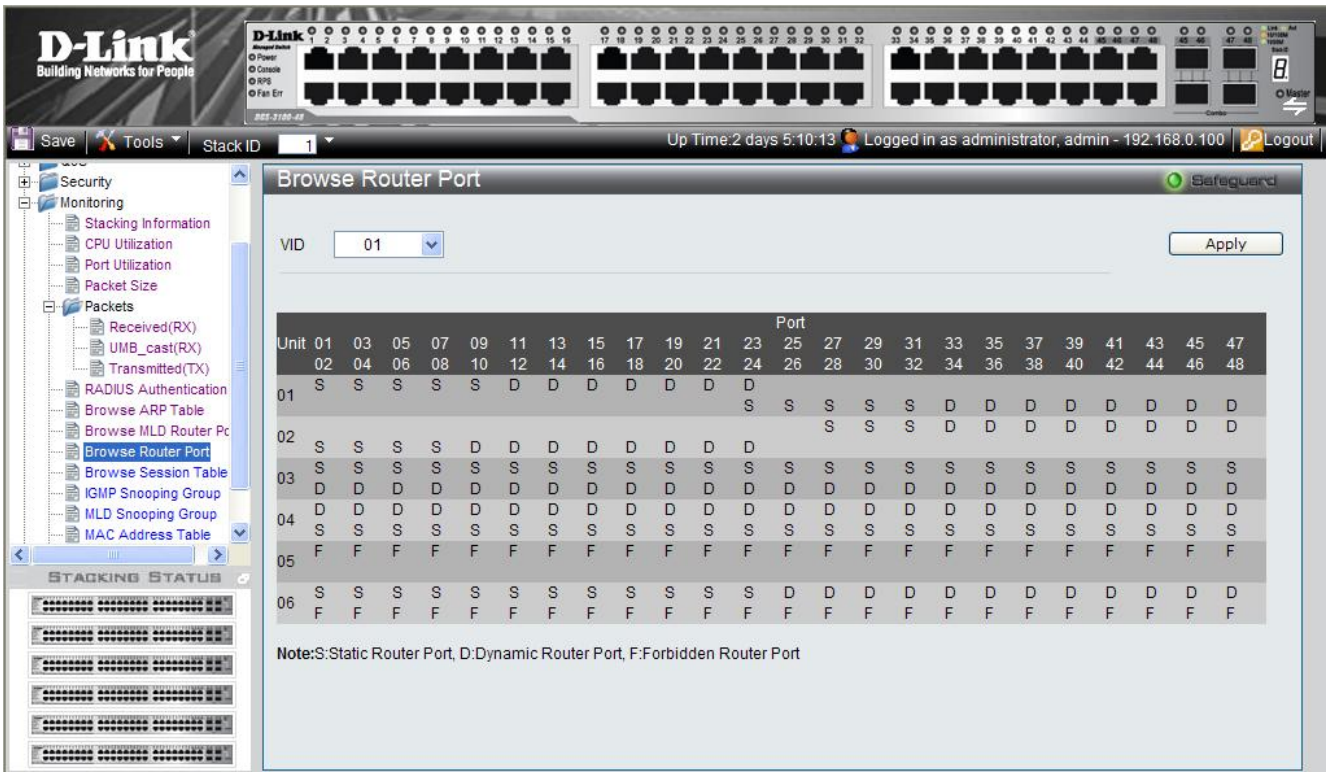


Figure 0-11 Browse Router Port Page

The Browse Router Port Page contains the following fields:

Field	Description
VID	Indicates the VLAN identification.
Unit	Indicates the stacking member for which the router ports information is displaying.
Port	Indicates the port for which the router port settings are displayed. Ports have the following settings: *S* — Indicates a static port. *D* — Indicates a dynamic port. *F* — Indicates a forbidden port.

2. Define the *VID* field.
3. Click Apply. The selected ports appear on the selected VLAN.

Viewing Session Table

The *Browse Session Table Page* displays information regarding device sessions which were initiated by system Users. To view session table information:

1. Click **Monitoring > Browse Session Table**. The *Browse Session Table Page* opens:

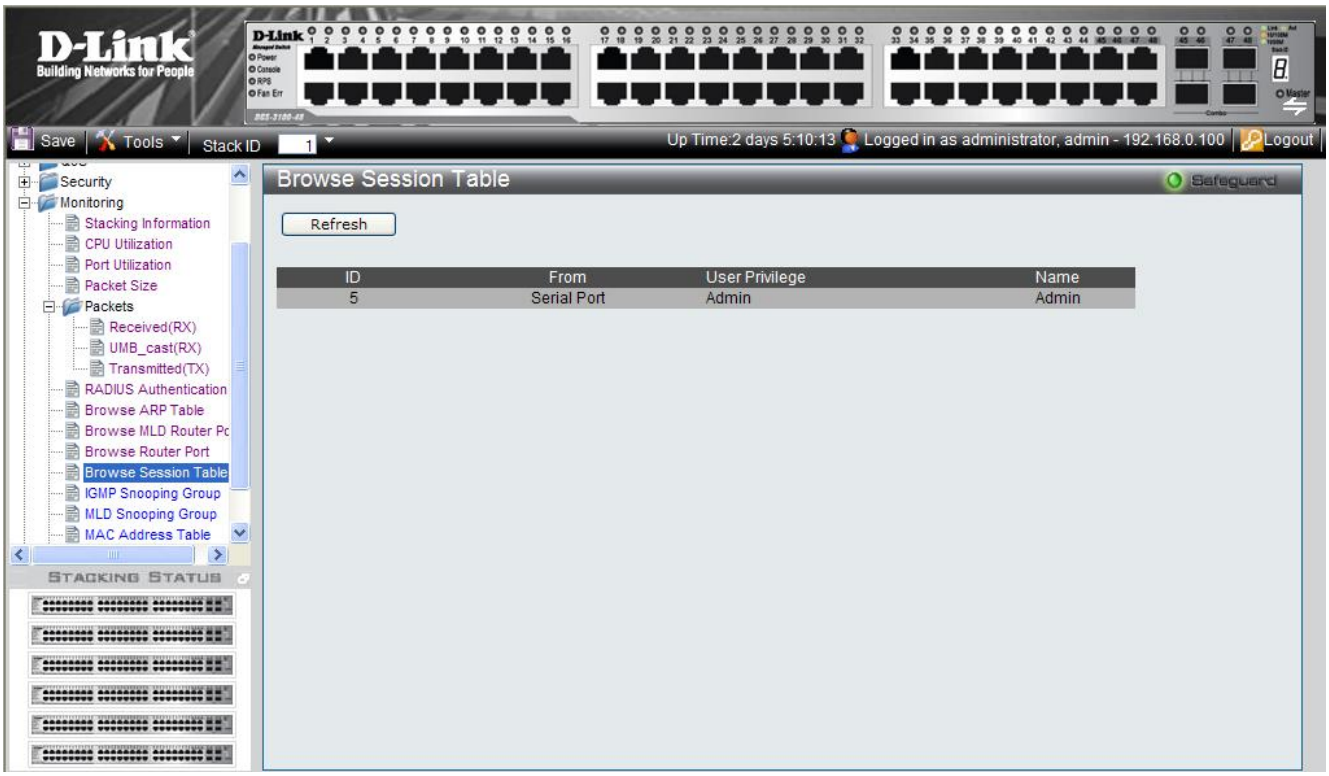


Figure 6-12 Browse Session Table Page

The Browse Session Table Page contains the following fields:

Field	Description
ID	Displays the browse session table entry.
From	Indicates the type of interface from which the system session was initiated.
User Privilege	Indicates the user privileged assigned to the user who imitated the system session.
Name	Displays the name of the user that initiated the system session.

Viewing IGMP Group Information

The *IGMP Snooping Group Page* contains vital IGMP group information, including the Multicast Group IP address and the corresponding MAC address through which the IGMP packets passed.

1. Click **Monitoring >IGMP Snooping Group**. The *IGMP Snooping Group Page* opens:

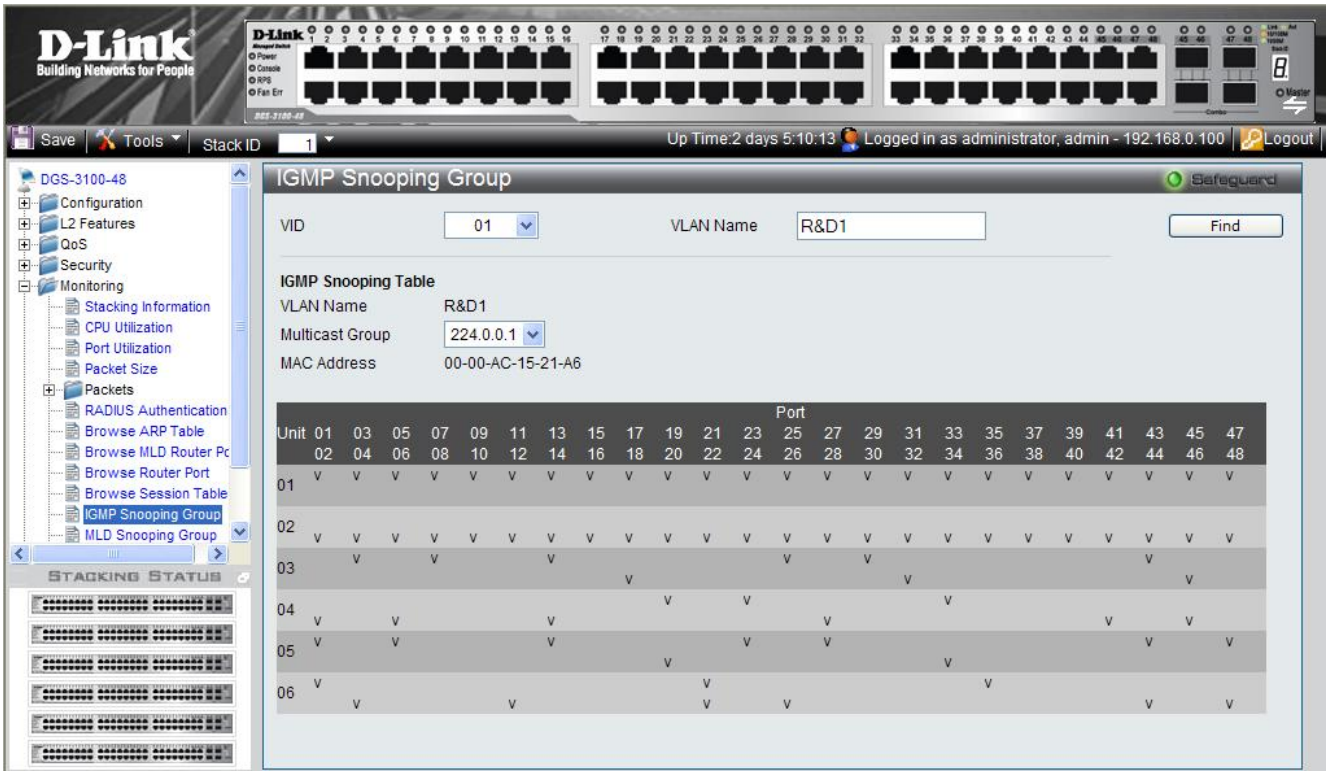


Figure 6-13 IGMP Snooping Group Page

The IGMP Snooping Group Page contains the following fields:

Field	Description
VID	Defines the VLAN ID for the IGMP Snooping Group.
VLAN Name	Defines the VLAN name.
VLAN Name	Displays the currently selected user-defined VLAN name.
Multicast Group	Displays the IP address assigned to the Multicast group.
MAC Address	Displays the MAC address assigned to the Multicast group.
Port	Displays the ports where the IGMP packets were snooped.

2. Define the VD and Vlan fields.
3. Click Find. The IGMP Snooping Group Page displays relevant information.

Viewing MLD Group Information

The *MLD Snooping Group Page* contains vital MLD group information, including the Multicast Group IP address and the corresponding MAC address through which the MLD packets passed.

1. Click **Monitoring > MLD Snooping Group**. The *MLD Snooping Group Page* opens:

Figure 6-114 MLD Snooping Group Page

The MLD Snooping Group Page contains the following fields:

Field	Description
VID	Defines the VLAN ID for the MLD Snooping Group.
VLAN Name	Defines the VLAN name.
VLAN Name	Displays the currently selected user-defined VLAN name.
Multicast Group	Displays the IP address assigned to the Multicast group.
MAC Address	Displays the MAC address assigned to the Multicast group.
Port	Displays the ports where the MLD packets were snooped.

2. Define the *VID* and *VLAN Name* fields.
3. Click Find. The *MLD Snooping Group Page* displays relevant information

Defining Dynamic and Static MAC Addresses

Packets addressed to destinations stored in either the Static or Dynamic databases are immediately forwarded to the port. The *MAC Address Table Page* can be sorted by interface, VLAN, or MAC Address, whereas MAC addresses are dynamically learned as packets from sources that arrive at the device. Static addresses are configured manually.

An address becomes associated with a port by learning the port from the frame's source address, however if a frame addressed to a destination MAC address is not associated with a port, that frame is flooded to all relevant VLAN ports. To prevent the Bridging table from overflowing, a dynamic MAC address, from which no traffic arrives for a set period, is erased.

To prevent static MAC addresses from being deleted when the device is reset, ensure that the port attached to the MAC address is locked.

1. Click **Monitoring > MAC Address Table**. The *MAC Address Table Page* opens:

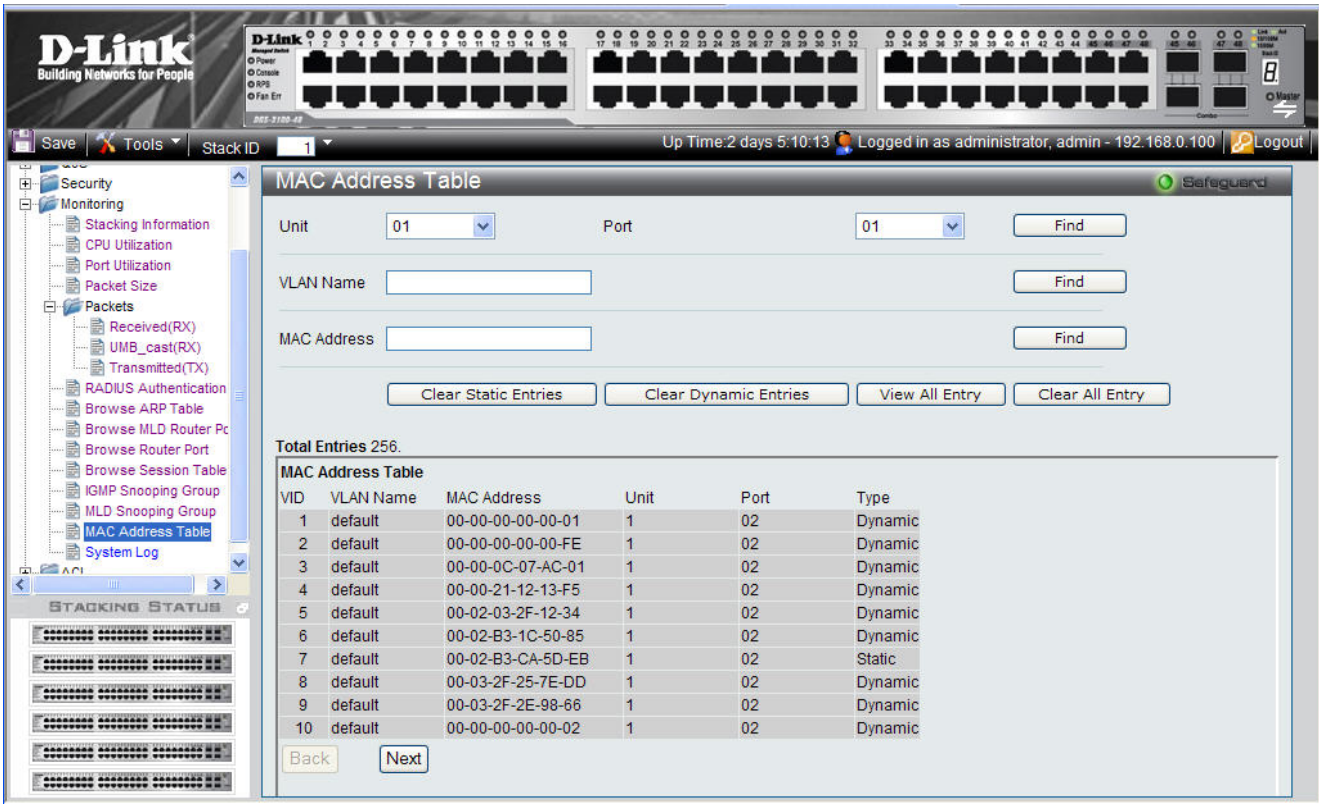


Figure 6-15 MAC Address Table Page

The MAC Address Table Page contains the following fields:

Field	Description
Unit	Displays the Stacking member Unit 1 for which the MAC address parameters are displayed.
Port	Defines the port for which the MAC address parameters are displayed.
VLAN Name	Defines the VLAN for which the MAC address parameters are displayed.
MAC Address	Displays the MAC address assigned to the port or VLAN.
VID	Displays the VLAN ID to which the MAC address is assigned.
Type	Indicates how the MAC was assigned. The possible values are: – Dynamic — Indicates that the MAC address is dynamically created. – Static — Indicates the MAC address is a static IP address.

2. Select the Stacking member in the Unit field.
3. Define the *Port*, *VLAN Name*, and *MAC Address* fields.

4. Click Find.
   - To view all entries, click View All Entry.
   - To clear static entries, click Clear Static Entries.
   - To clear dynamic entries, click Clear Dynamic Entries.
   - To clear all entries, click Clear All Entry. The MAC Address Table updates and displays total entries.
   - To scroll down the table, click Next.
   - To scroll up the table, click Back.

Viewing System Log

The *System Log Page* provides information about system logs, including information when the device was booted, how the ports are operating, when users logged in, when sessions timed out, as well as other system information. To view the *System Log Page*:

1. Click **Monitoring > System Log**. The *System Log Page* opens:

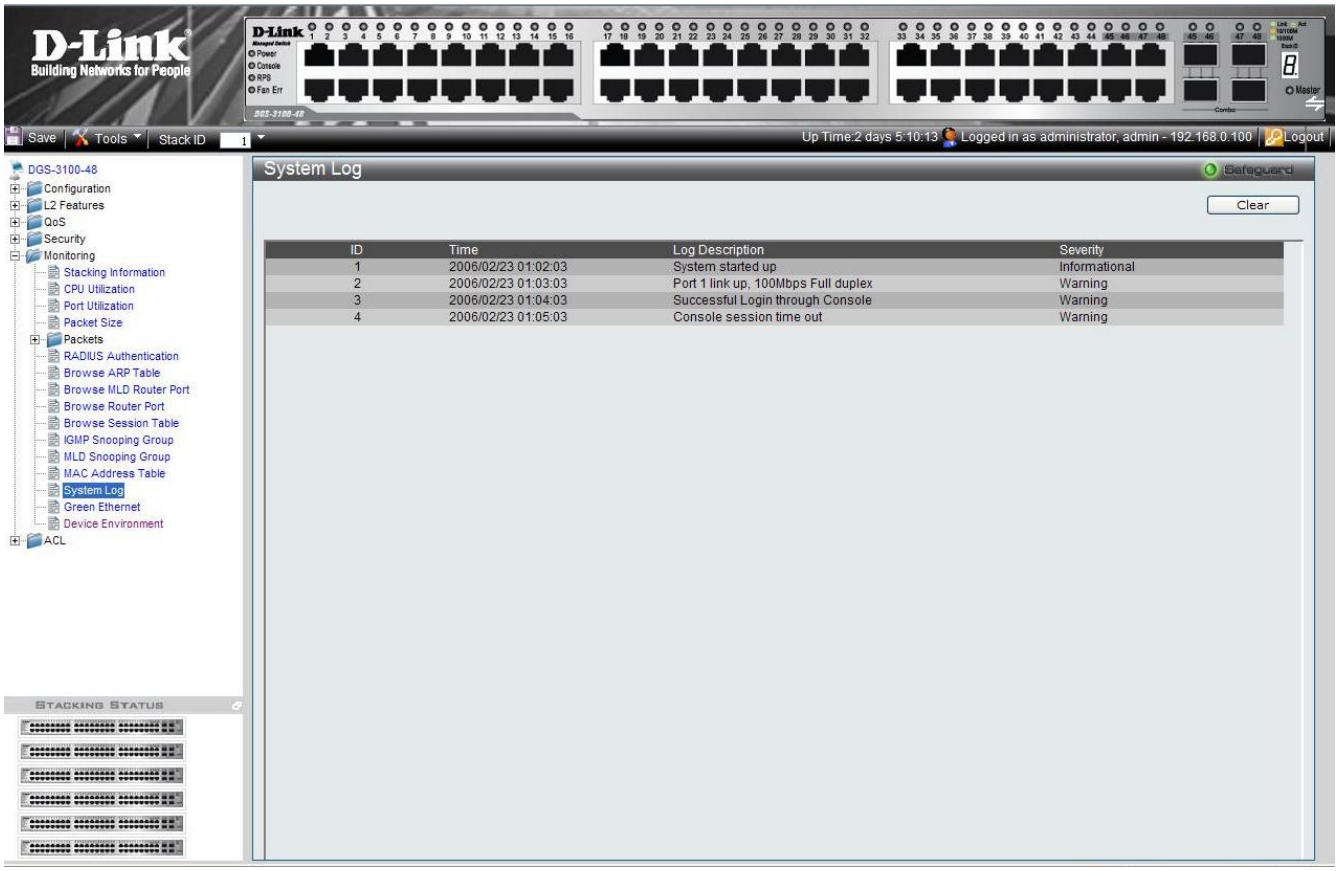


Figure 6-16 System Log Page

The System Log Page contains the following fields:

Field	Description
ID	Displays the system log table entry.
Time	Displays the time in days, hours, and minutes the log was entered in the Switch History Log Table.
Log Description	Displays a description event recorded in the *System Log Page*.
Severity	The following are the available log severity levels: – Warning — The lowest level of a device warning. The device is functioning, but an operational problem has occurred. – Informational — Provides device information.

To clear the log:

2. Click Clear. The System Log Page is cleared.

Green Ethernet

Green Ethernet improves the energy consumption of the switch by providing a power saving technology that automatically reduces power consumption upon detection of short cables (less than 40 meters) or *Link Down*. This is accomplished without forfeiting network integrity.

To enable Green Ethernet:

1. Click **Monitoring > Green Ethernet**. The *Green Ethernet Page* opens:

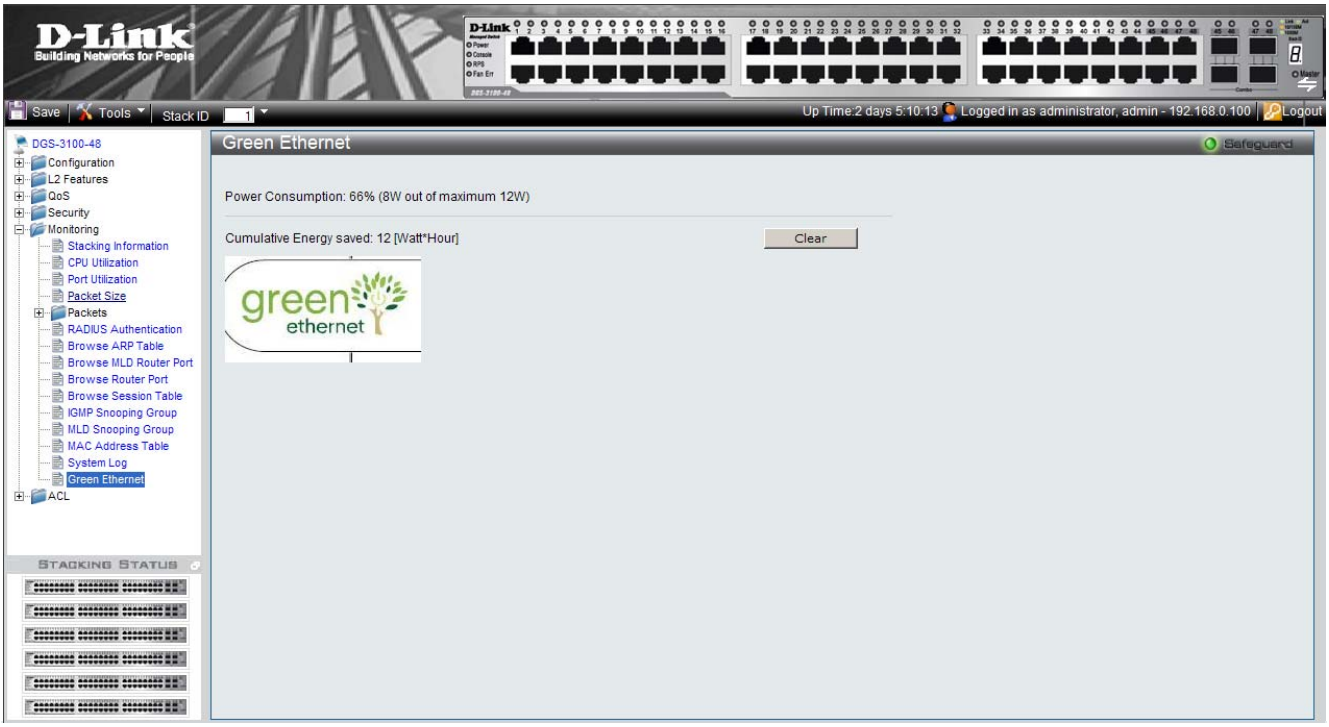


Figure 0-12 Green Ethernet Page

The Green Ethernet Page contains the following fields:

Field	Description
Power Consumption	Displays the device power consumption. The power consumption is displayed in percentage as well as in Watts.
Cumulative Energy saved	Displays the cumulative power conserved by using Green Ethernet.

2. To clear the Cumulative Energy saved value:
3. Click Clear. The Cumulative Energy saved is cleared.

Device Environment

Device Environment displays basic information regarding the operating environment of the device in areas such as temperature and ventilation.

To view Device Environment:

1. Click **Monitoring > Device Environment**. The *Device Environment Page* opens:

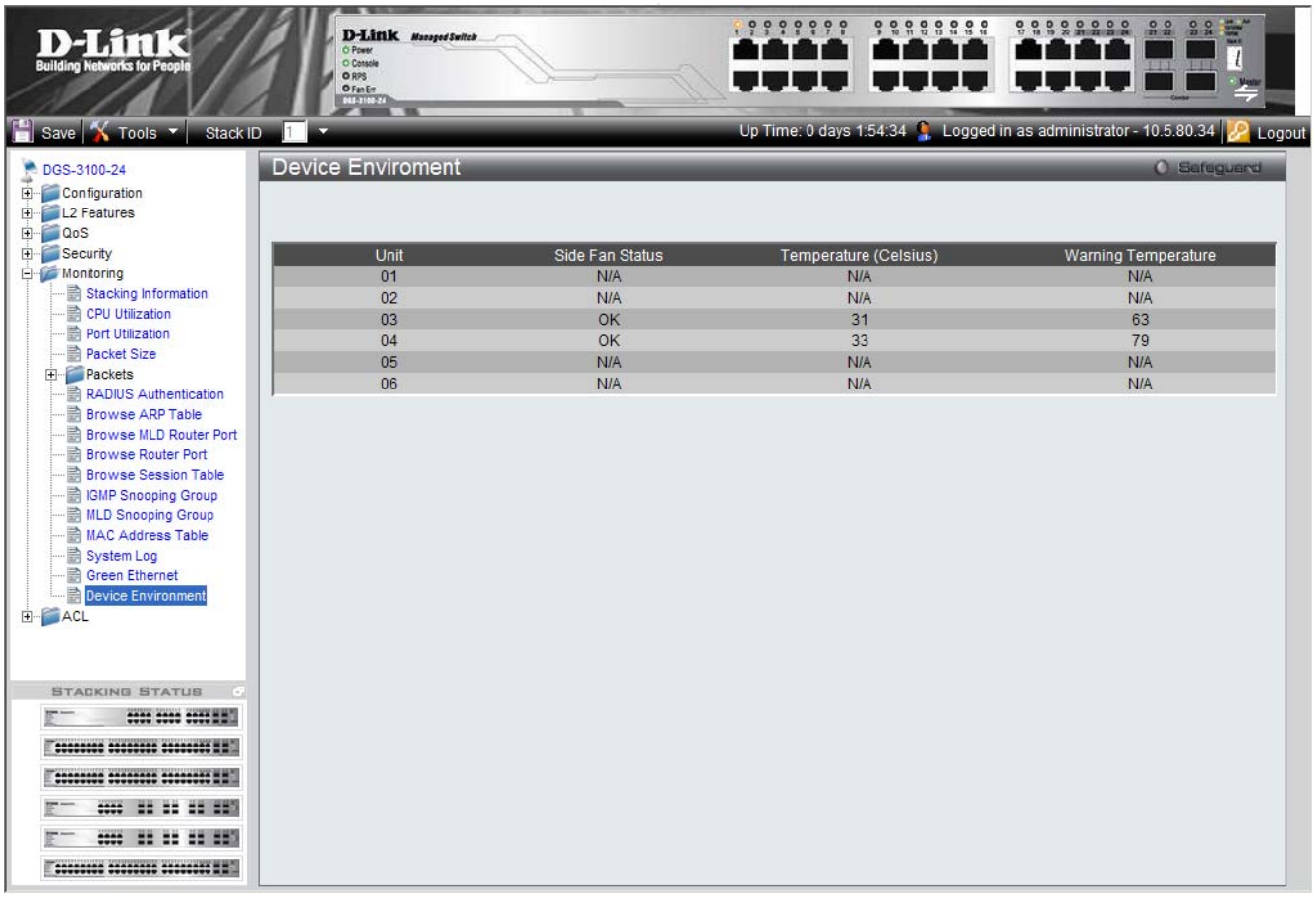


Figure 0-13 Device Environment Page

The Device Environment Page contains the following fields:

Field	Description
Unit	Indicates the stacking member for which the device environment is displayed.
Side Fan Status	Displays the side fan status. The possible values are: – OK — Indicates the fan is operating normally. – Fail — Indicates the fan is not operating normally. – N/A — Indicates a fan is not installed on the device.
Temperature	The current temperature of the device. Each device type has a different Warning Temperature, N/A means that the device HW revision does not support temperature reading.
Warning Temperature	The maximum allowed operating temperature of the device.

Errors

The Error pages display various types of error counters for received and transmitted packets.

Errors in Received Packets

To view Rx errors:

1. Click **Monitoring > Errors > Received (Rx)**. The *Received (Rx) Page* opens**:**

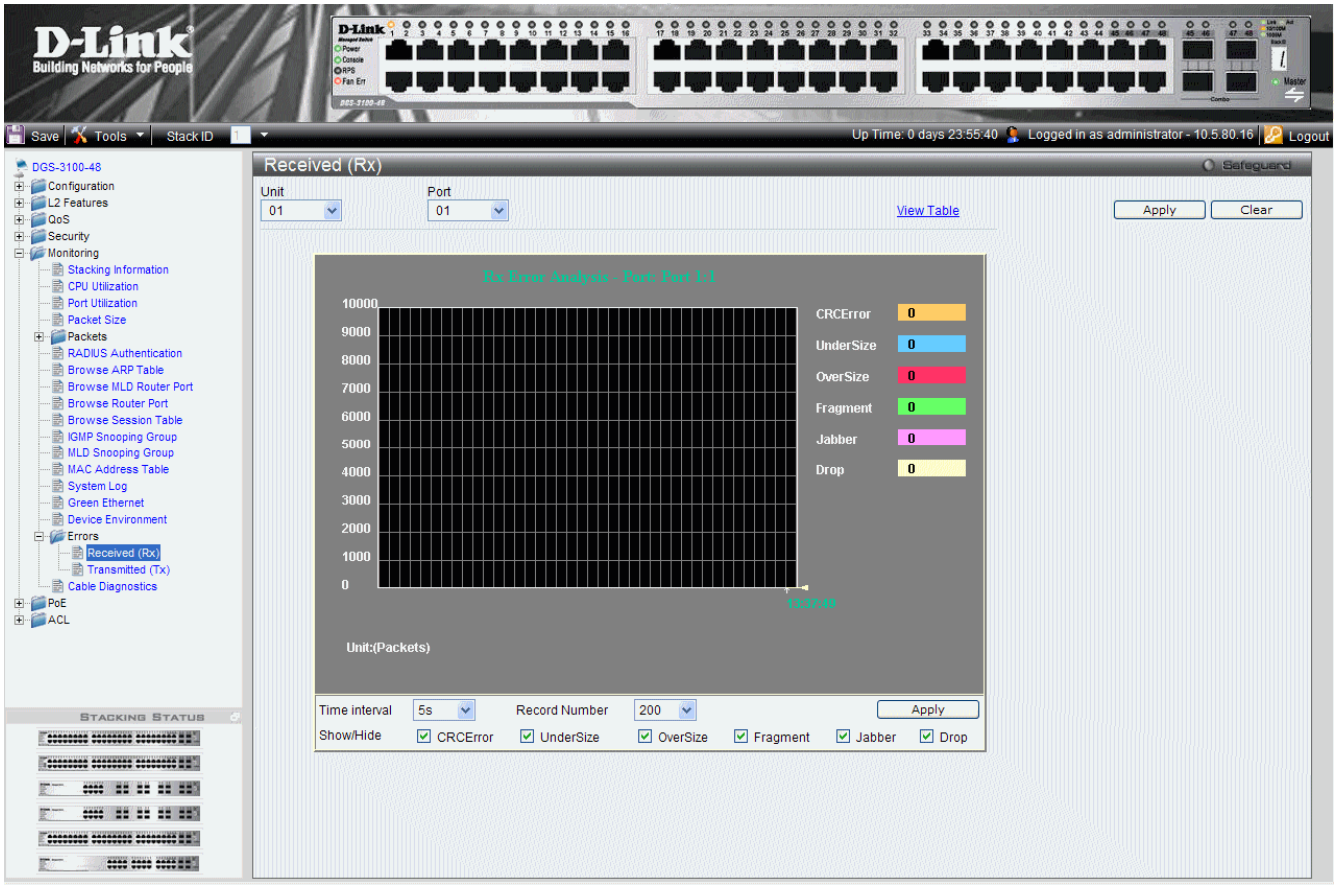


Figure 0-14 Received Rx Page

The Received (Rx) Page contains the following fields:

Field	Description
Unit	Indicates the stacking member for which the error counters are displayed.
Port	Indicates the port for which the error counters are displayed.
Time Interval	Indicates the time interval for which packets are displayed. The possible field values are: 1s - 5s, 10s, 15s, 20s, 30s, 40s, 50s, and 60s.
Record Number	Indicates the transmitted record number.
CRCError	Displays the number of packets received whose length (excluding framing bits, but including FCS octets) was between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
UnderSize	Displays the number of packets received that were shorter than 64 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

Field	Description
OverSize	Displays the number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragment	Displays the number of packets received that were shorter than 64 octets (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Jabber	Displays the number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Drop	Displays the number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times that this condition was detected.

2. Select a unit and port and click Apply. Information for the selected port in the selected unit is displayed.
3. Click View Table to see the results in table format.
4. Enter Time Interval, Record Number and the types of error counters that you want to display.
5. Click Apply. The information is displayed.

Errors in Transmitted Packets

To view Tx errors:

1. Click **Monitoring > Errors > Transmitted (Tx)**. The *Transmitted (Tx) Page* opens:

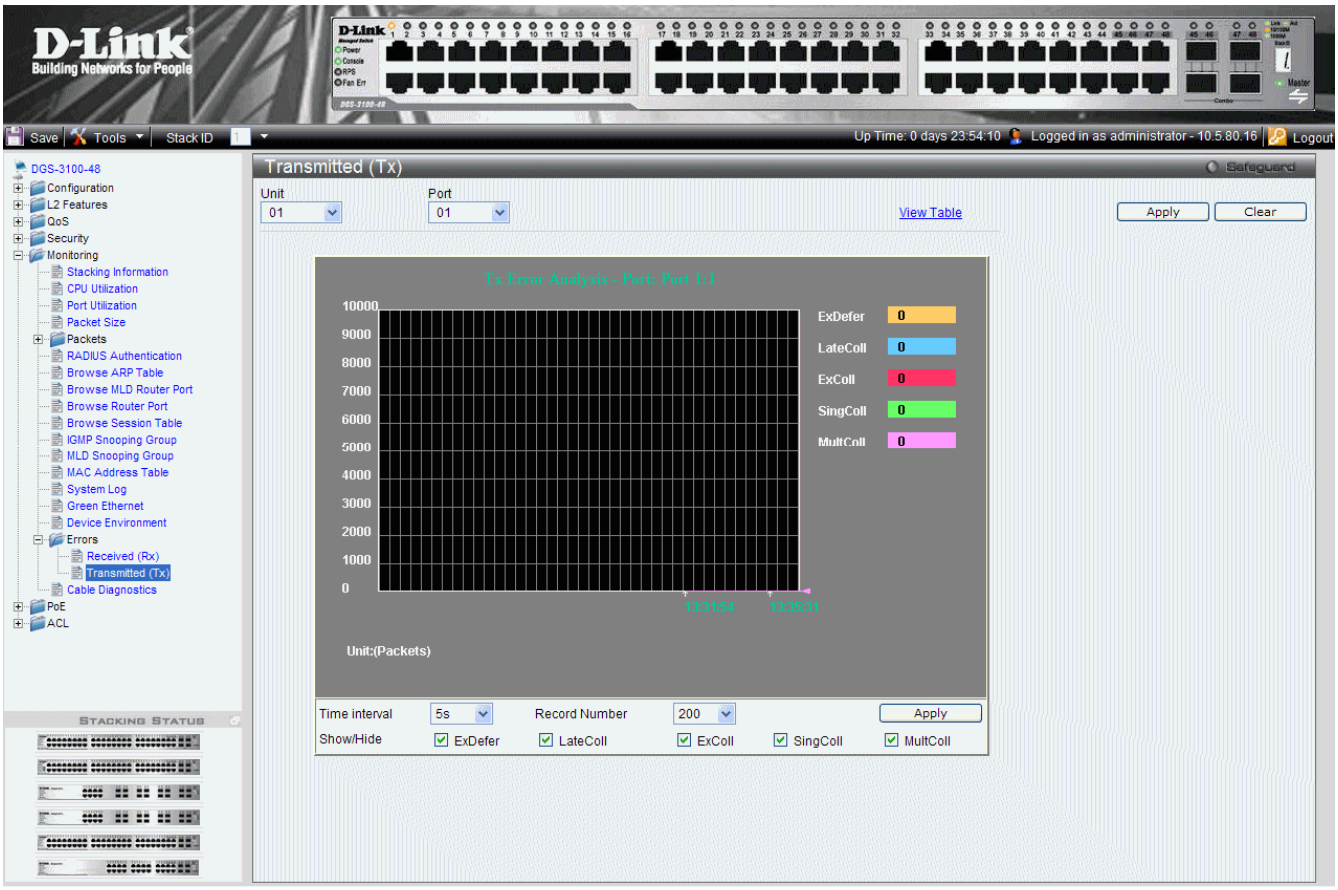


Figure 0-15 Transmitted Tx Page

The Received (Rx) Page contains the following fields:

Field	Description
Unit	Indicates the stacking member for which the device environment is displayed.
Port	Displays error counters for the selected port.
Time Interval	Indicates the time interval for which packets are displayed. The possible field values are: 1s - 5s, 10s, 15s, 20s, 30s, 40s, 50s, and 60s.
Record Number	Indicates the transmitted record number.
exDefer	Displays the number of frames for which the first transmission attempt is delayed because the medium is busy.
LateColl	Displays the number of times that a collision is detected later than one time slot into the transmission of a packet.
ExColl	Displays the number of frames for which transmission fails due to excessive collisions.
SingColl	Displays the number of frames that are involved in a single collision, and are subsequently transmitted successfully
MultColl	Displays the number of frames that are involved in more than one collision and are subsequently transmitted successfully.

2. Select a unit and port and click Apply. Information for the selected port in the selected unit is displayed.
3. Click View Table to see the results in table format.
4. Enter Time Interval, Record Number and the types of error counters that you want to display. Click Apply. The information is displayed.

Cable Diagnostics

The *Cable Diagnostics* Page contains fields for performing tests on copper cables. Cable testing provides information about where errors occurred in the cable, the last time a cable test was performed, and the type of cable error which occurred. The tests use Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port. Cables up to 140 meters long can be tested. Cables are tested when the ports are in the down state, with the exception of the Approximated Cable Length test. The cable length returned is an approximation in the ranges of less than 50 meters, 50m-80m, or 80m-100m. The deviation may be up to 20 meters. To run the Cable Diagnostics:

1. Click **Monitoring > Cable Diagnostics**. The *Cable Diagnostics Page* opens**:**

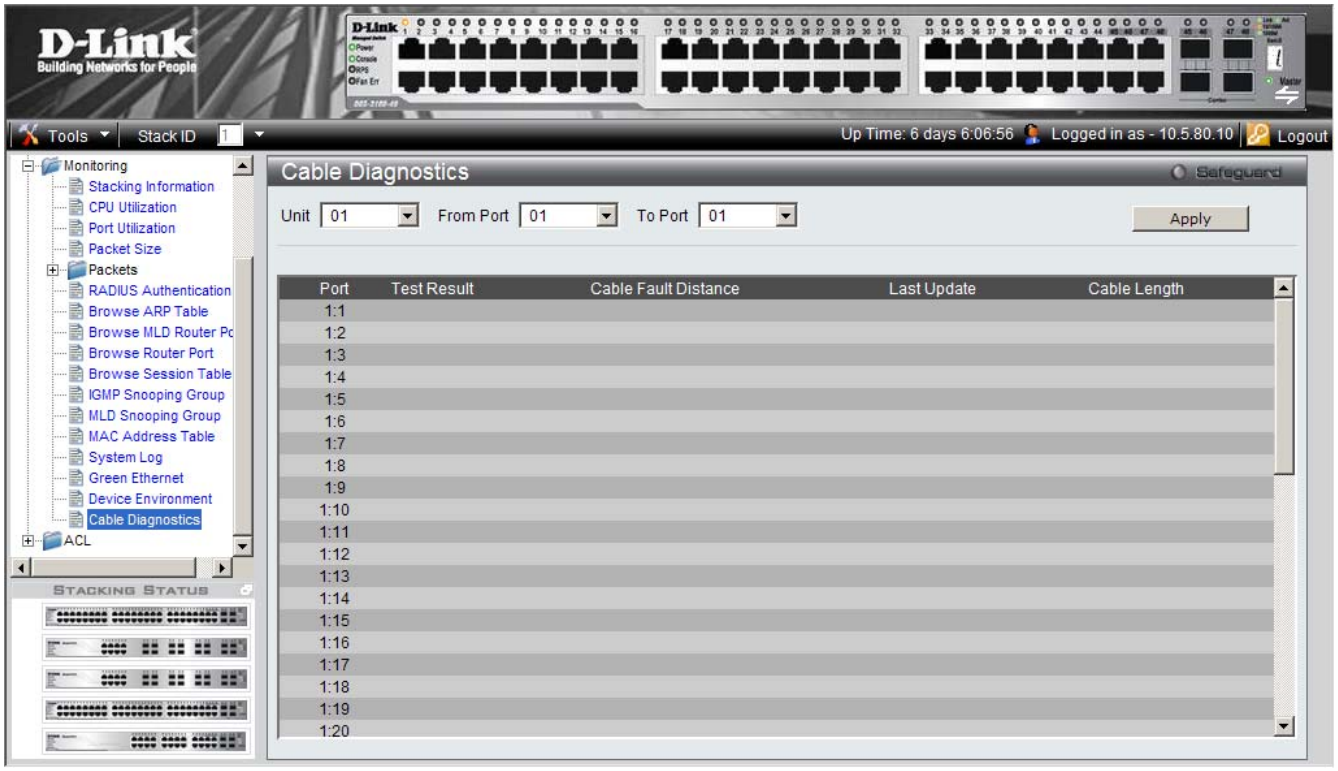


Figure 6-16 Cable Diagnostics Page

The Cable Diagnostics Page contains the following fields:

Fields	Description
Unit	Defines the stacking member for which the port settings are displayed.
From Port	Defines the port number from which the diagnostics will apply.
To Port	Defines the port number to which ports the diagnostics will apply.
Port	Lists the ports to be tested.
Test Result	The cable test results. Possible values are: • No Cable — A cable is not connected to the port. Whether the fiber is connected to the port or not. • Open Cable — A cable is connected on only one side. • Short Cable — A short has occurred in the cable. • OK — The cable passed the test.
Cable Fault Distance	The distance from the port where the cable error occurred.
Last Update	The last time the port was tested.
Cable Length	The approximate cable length. This test can only be performed when the port is up and operating at 1 Gbps.

2. Ensure that both ends of the copper cable are connected to a device.
3. Define the *Unit*, *From Port*, and *To Ports* fields.
4. Click Apply. The diagnostic tests are carried out and the list is updated.

7

MANAGING POWER OVER ETHERNET DEVICES

NOTE: This chapter is valid only when using devices on which Power over Ethernet (PoE) is supported.

Power over Ethernet (PoE) provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power-over-Ethernet removes the necessity of placing network devices next to power sources. Power-over-Ethernet can be used in the following applications:

- IP Phones
- Wireless Access Points
- IP Gateways
- Audio and Video Remote Monitoring

Powered Devices are devices that receive power from the device power supplies, for example IP phones. Powered Devices are connected to the device via Ethernet ports. Guard Band protects the device from exceeding the maximum power level. For example, if 400W is the maximum power level, and the Guard Band is 20W, if the total system power consumption exceeds 380W no additional PoE components can be added. The accumulated PoE components power consumption is rounded down for display purposes.

This section includes the following topics:

- Defining PoE Port Information
- Configuring PoE System

Defining PoE Port Information

The PoE Port Setting Page contains information about the system's CPU utilization.

1. Click **PoE > PoE Port Setting**. The *PoE Port Setting Page* opens:

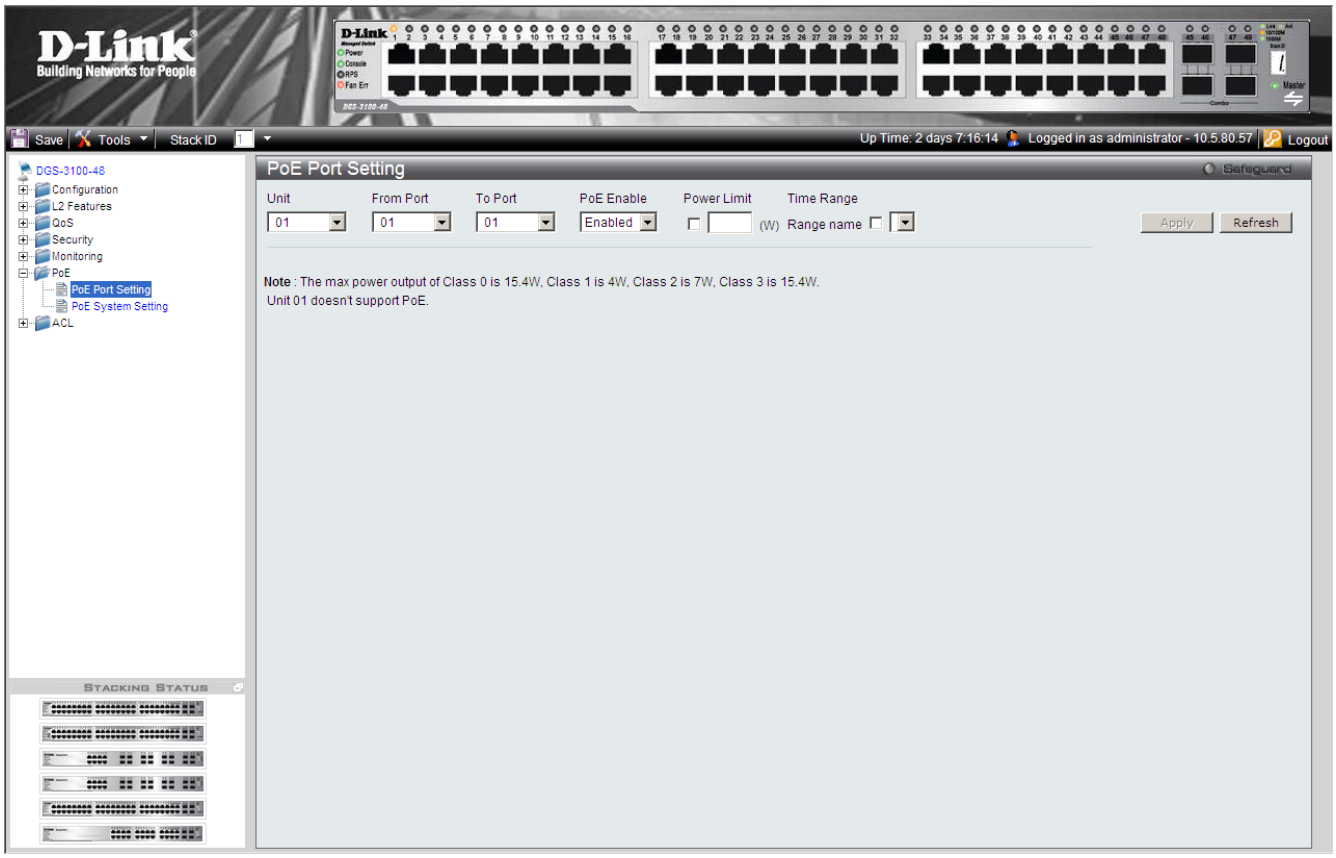


Figure 0-1 PoE Port Setting Page

The PoE Port Setting Page contains the following fields:

Fields	Description
Unit	Defines the stacking member for which the PoE settings are displayed.
From Port	Defines the port number from which the PoE settings will apply.
To Port	Defines the port number to which ports the PoE settings will apply.
PoE Enable	Indicates if PoE is enabled on the interface. The possible field values are: *Enabled* —PoE is enabled on the ports. This is the default value. *Disabled* —PoE is disabled on the ports.
Power Limit	Defines whether a Power Limit will be set. This enables saving power when the PoE devices are typically not in use. The possible field values are: • *Unchecked* — The Power Limit Time Range is disabled on the ports. This is the default value. • *Checked* — The Power Limit Time Range is enabled on the ports.
Time Range Name	Defines a preset time range. Specific Time Ranges can be defined in the Time Range Setting Page. This field is only active if the selected unit supports PoE.
Power Limit	Defines whether a Power Limit will be set. This enables saving power when the PoE devices are typically not in use. The possible field values are: • *Unchecked* — The Power Limit Time Range is disabled on the ports. This is the default value. • *Checked* — The Power Limit Time Range is enabled on the ports.

2. Define the Unit, From Port, To Port, and PoE Enable fields.
3. Define the Power Limit and Time Range Name fields.
4. Click Apply. The PoE Port Settings are saved, and the device is updated.

Configuring PoE System Settings

The *PoE System Setting Page* contains port utilization information for specific ports. To view port statistics:

1. Click **PoE > PoE System Setting**. The *PoE System Setting Page* opens:

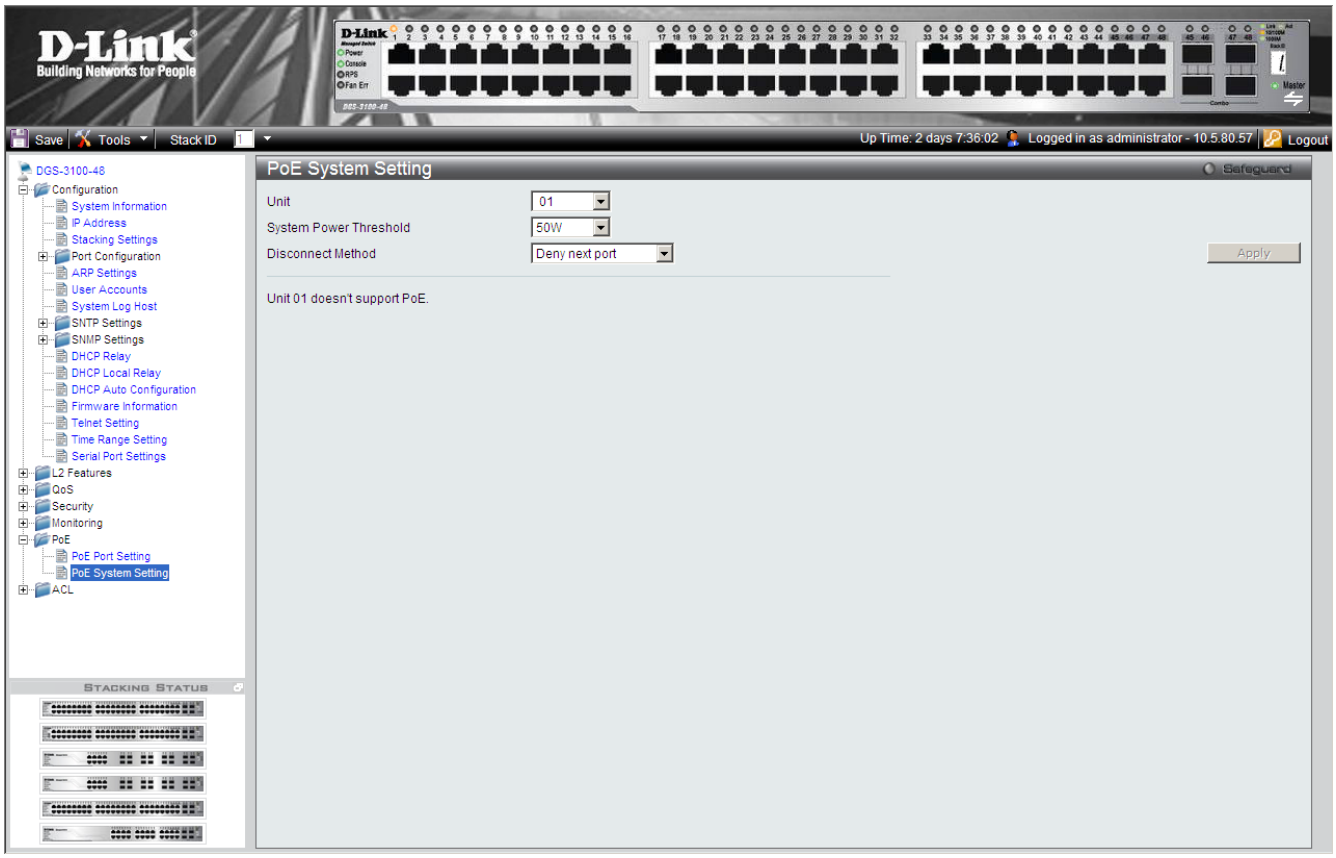


Figure 0-2 PoE System Setting Page

The PoE System Setting Page contains the following fields:

Fields	Description
Unit	Defines the unit number.
System Power Threshold	Indicates the power in Watts consumed before an alarm is generated. The possible field values are: *50W* — Indicates 50 watts. *100W* — Indicates 100 watts. *170W* — Indicates 170 watts.
Disconnect Method	Defines the method used to deny power to a port once the threshold is reached. The possible fields are: *Deny next port* —Denies power to the next port that makes a PoE request after the threshold has been reached. This is the default value. *Deny Low priority port*—Denies power to the lowest-priority port after the threshold has been reached.

8

DEFINING ACCESS PROFILE LISTS

Access Control Lists (ACL) allow network managers to define classification actions and rules for specific ingress ports. Packets entering an ingress port with an active ACL are either admitted, denied or subject to Quality of Service action.

For example, a network administrator defines an ACL rule that states port number 20 can receive TCP packets, however, if a UDP packet is received, the packet is dropped.

Access Profiles and Access Rules that are made of the filters determine traffic classifications.

This section cotains the following topics:

- Methods for Defining Access Control Lists
- ACL Configuration Wizard
- Defining Access Profile Lists
- Finding ACL Rules

Methods for Defining Access Control Lists

Access Control Lists (ACLs) can be configured in the DGS-3100 series via the WEB GUI in either of the following ways:

- ACL Configuration Wizard — This feature automatically creates both Access Profiles and their rules. After the system creates an Access Profile and an Access Rule, it binds it to a port/LAG or a group of ports/LAG. Each operation via the Wizard can create either a MAC-based ACL or IP-based ACL. The user cannot combine both types of ACLs in the same operation. This feature is described below.
- ACL Profile List — This feature is used to manually create profiles and rules. This feature is described in the Defining Access Profile Lists section.

ACL Configuration Wizard

The *ACL Configuration Wizard* Page provides information for configuring Access Control Lists. The ACL Configuration Wizard Page assists in configuring ACLs intuitively and quickly, and creates ACL profiles and rules automatically. To define ACLs:

1. Click **ACL > ACL Configuration Wizard**. The *ACL Configuration Wizard Page* opens:

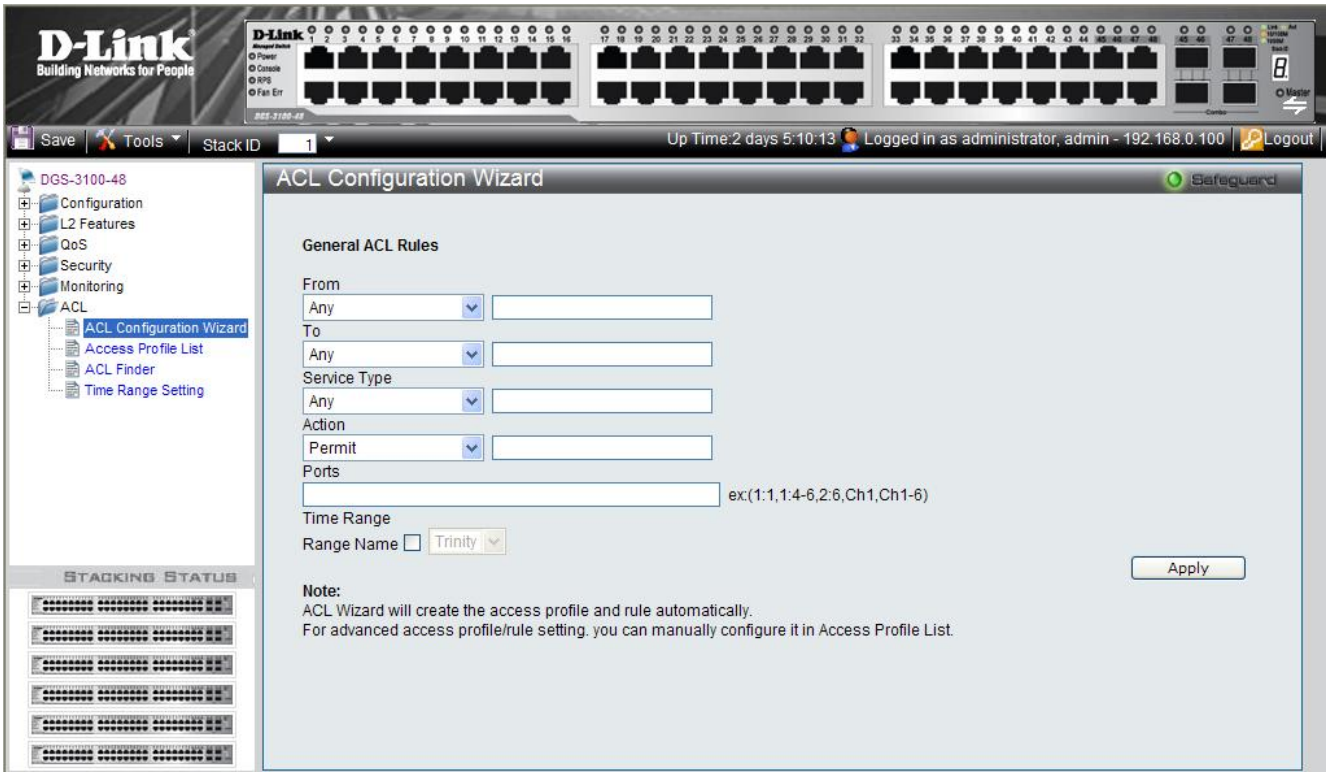


Figure 0-1 ACL Configuration Wizard Page

The ACL Configuration Wizard Page contains the following fields:

Fields	Description
From	Defines the origin of accessible packets. The possible values are: *Any* — Indicates ACL action will be on packets from any source. *MAC Address* — Indicates ACL action will be on packets from this MAC address. *IPv4 Addresses* — Indicates ACL action will be on packets from this IPv4 source address. *IPv6 Addresses* — Indicates ACL action will be on packets from this IPv6 source address.
To	Defines the destination of accessible packets. The possible values are: *Any* — Indicates ACL action will take placed for packets with any destination. *MAC Address* — Indicates ACL action will take place for packets to this MAC address only. *IPv4 Addresses* — Indicates ACL action will take place on packets to this IPv4 address. *IPv6 Addresses* — Indicates ACL action will take place on pakets to this IPv6 address.
Service Type	Defines the type of service. The possible values are: *Any* — Indicates ACL action will take place for packets of all service types. *Ethertype* — Specifies Ethertype packet filtering. *ICMP All* — Specifies an ICMP packets filtering *IGMP* — Specifies an IGMP packets filtering *TCP ALL* — Specifies an TCP packets filtering

Fields	Description
	TCP Source Port — Matches the packet to the TCP Source Port *TCP Destination Port* — Matches the packet to the TCP Destination Port *UDP All* — Specifies a UDP Packets filtering. *UDP Source Port* — Matches the packet to the UDP Source Port *UDP Destination Port* — Matches the packet to the UDP Destination Port
Action	Defines the ACL forwarding action matching the rule criteria. The possible values are: *Permit* — Forwards packets if all other ACL criteria are met. *Deny* — Drops packets if all other ACL criteria is met. *Rate Limiting* — Rate limiting is activated if all other ACL criteria is met. *Change 1p Priority* — VPT (CoS) value is changed if all other ACL criteria is met. *Replace DSCP* — Reassigns a new DSCP value to the packet if all other ACL criteria are met.
Ports	Defines ports to be configured. An example of possible values is: 1:1, 1:4-6, and 2:6.
Time Range	Specifies whether the configured ACL is time-based.
Range Name	Selects the user-defined time range name to apply to the configured ACL.

2. Define the *From*, *To*, *Service Type*, *Action*, and *Ports* fields.
3. To configure a time-based ACL, Check the *Time Range* box and select the *Range Name* from the list.
4. Click Apply. The ACLs are configured, and the device is updated.

For advanced ACL setting please see the section below**.**

Defining Access Profile Lists

This section contains the following topics:

- Adding Access Rules
- Adding ACL Profiles
- Defining Layer 2 ACL
- Defining Layer 3 IPv4 ACL
- Defining Layer 3 IPv6 ACL
- Adding Access Rules

Adding ACL Profiles

The *ACL Profile List Page* provides information for configuring ACL Profiles manually. ACL profiles are attached to interfaces, and define how packets are forwarded if they match the ACL criteria.

1. Click **ACL > Access Profile List**. The *ACL Profile List Page* opens**:**

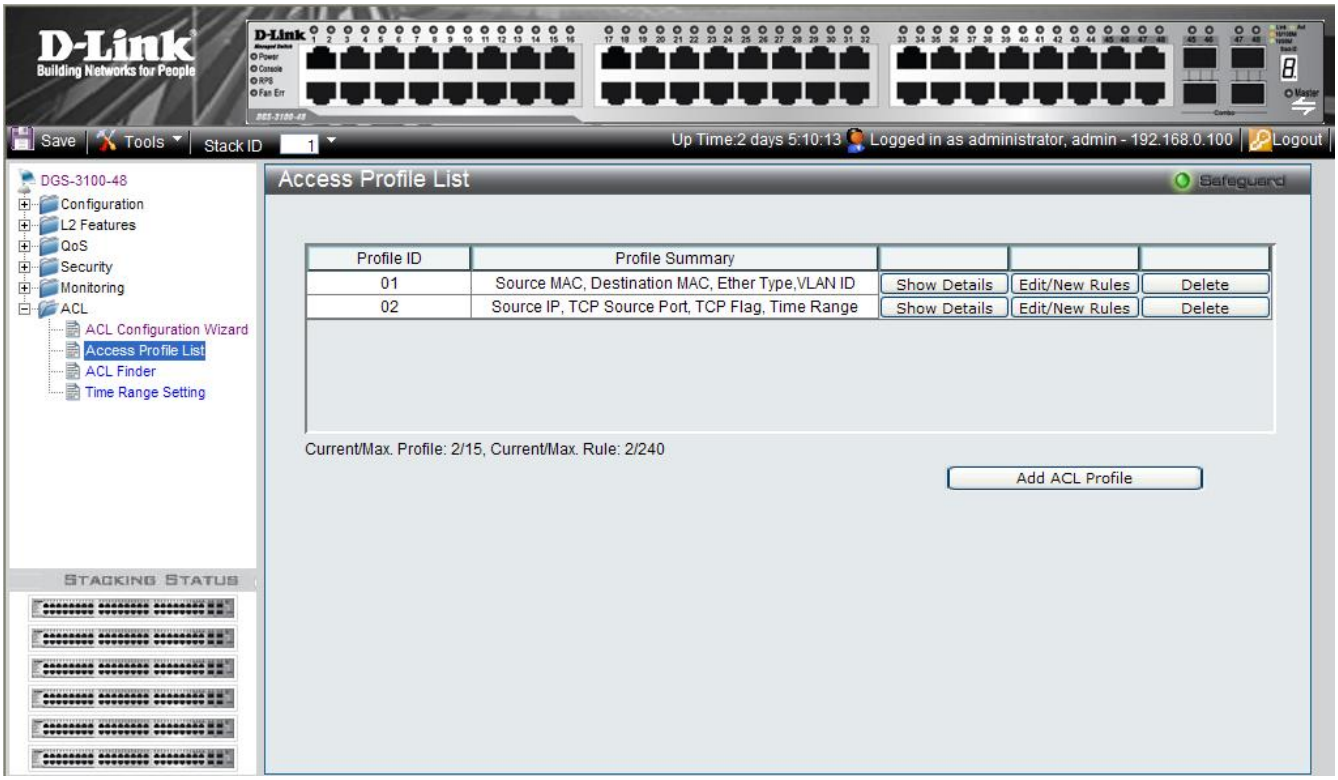


Figure 0-2 ACL Profile List Page

The ACL Profile List Page contains the following fields:

Field	Description
Profile ID	Displays the profile Identification number.
Profile Summary	Displays the access rule.

2. To display an ACL's profile details, click Show Details. The ACL profile details are displayed below the ACL table.
3. To define or show an access rule, click Edit/New Rules. The *Add Access Rule Page* opens. (See 'Defining Access Rules Lists' section, below.)
4. To delete an ACL profile, click Delete. The ACL profile is deleted.

5. To add an ACL profile Click Add ACL Profile. The *Add ACL Profile Page* opens:

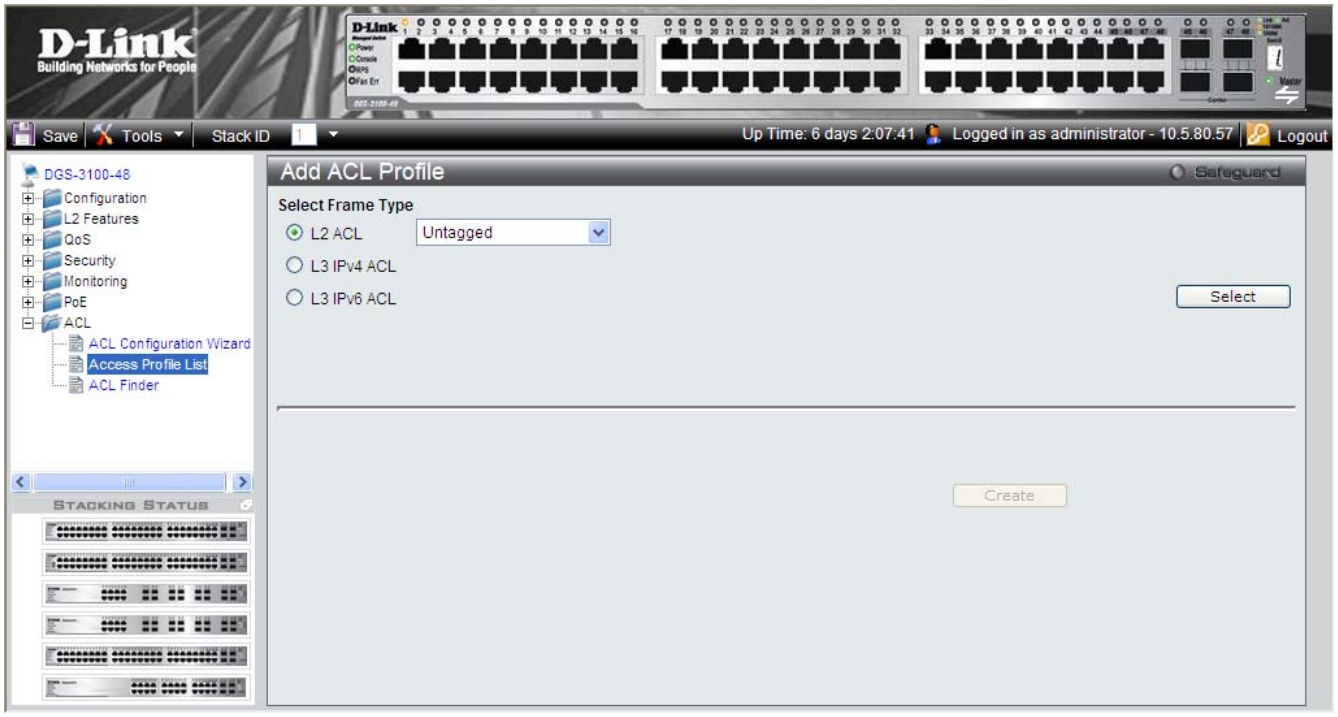


Figure 0-3 Add ACL Profile Page

The Add ACL Profile Page contains the following fields:

Field	Description
L2 ACL	Defines the ACL profile Layer 2 protocols. The possible values are: *Tagged* — Defines the profile Layer 2 to match 802.1Q fields in the Layer 2 header. *Untagged* — Defines the profile Layer 2 to check the Layer 2 header without the 802.1Q fields .
L3 IPv4 ACL	Defines the ACL profile Layer 3 protocols. The possible fields are: *ICMP* — Specifies ICMP as the Layer 4 protocol that the access profile checks. *IGMP* — Specifies IGMP as the Layer 4 protocol that the access profile checks *TCP* — Specifies TCP as the Layer 4 protocol that the access profile checks. *UDP* — Specifies UDP as the Layer 4 protocol that the access profile checks.
L3 IPv6 ACL	Defines the IPv6 ACL profile Layer 3 IPv6 protocols. The possible fields are: *ICMP* — Specifies ICMP as the Layer 3 IPv6 protocol that the access profile checks. *TCP* — Specifies TCP as the Layer 3 IPv6 protocol that the access profile checks. *UDP* — Specifies UDP as the Layer 3 IPv6 protocol that the access profile checks.

1. Define the *L2 ACL* or *L3 ACL* fields.
2. Click Select. The *Add ACL Profile Page* **updates accordingly,** enabling selection of the packet field to create filtering masks**.**

Defining Layer 2 ACL

If *L2 ACL* *Tagged* is selected, the page updates as follows:

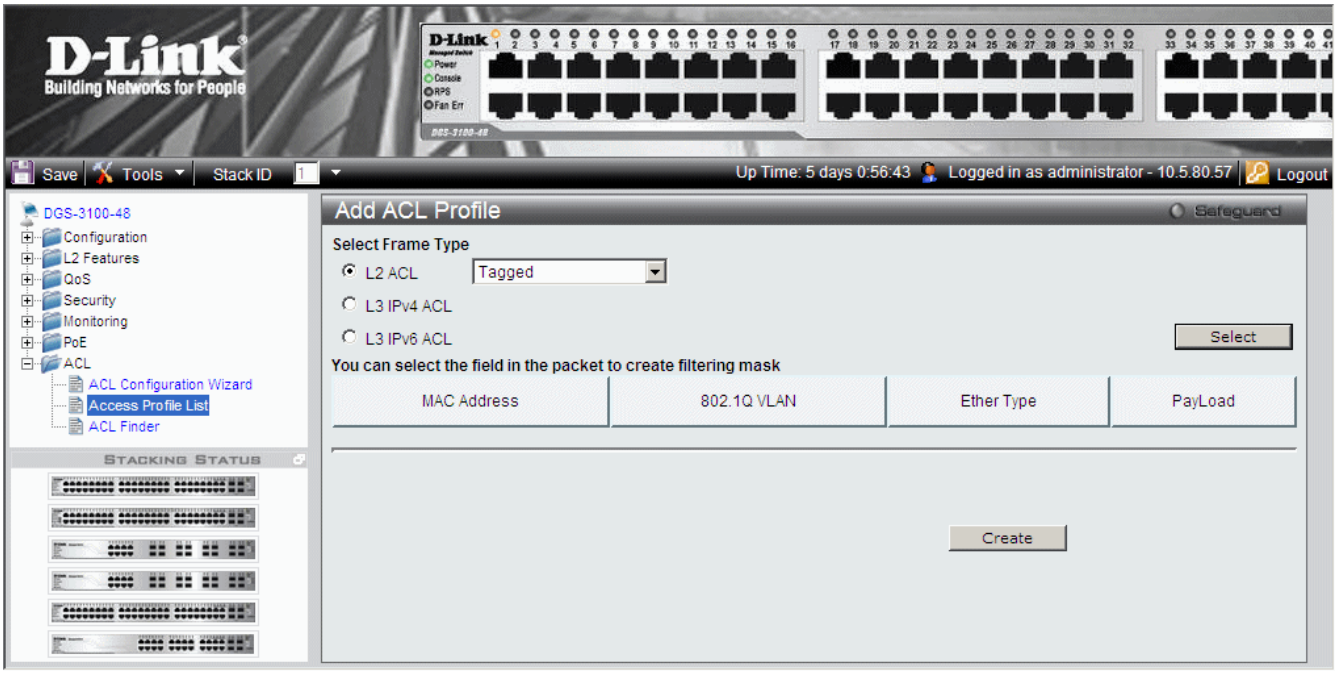


Figure 0-4 ACL Profile L2 ACL Tagged Page

If *L2 ACL* *Untagged* is selected, the page updates as follows:

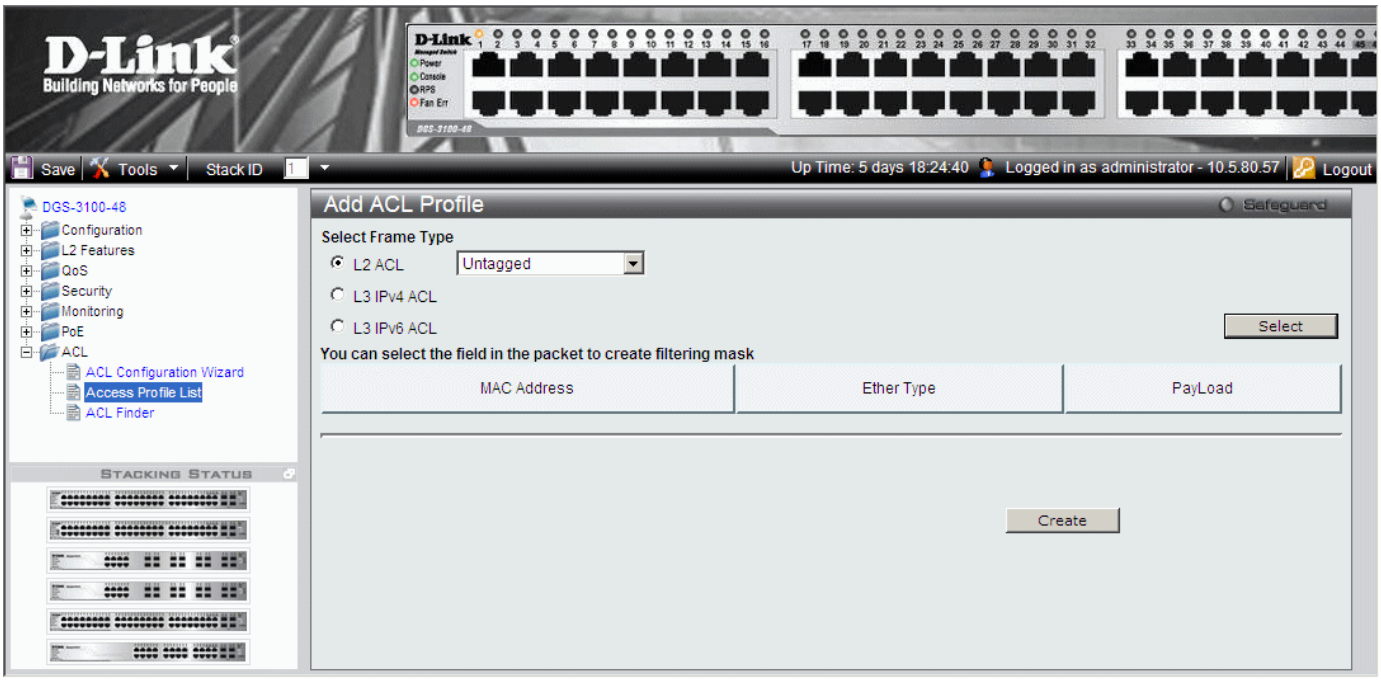


Figure 0-5 ACL Profile L2 ACL Untagged Page

To define L2 MAC Address ACL profile:

1. Click the *MAC Address* button. The *ACL Profile L2 ACL Tagged MAC Address Page* updates to show the following:

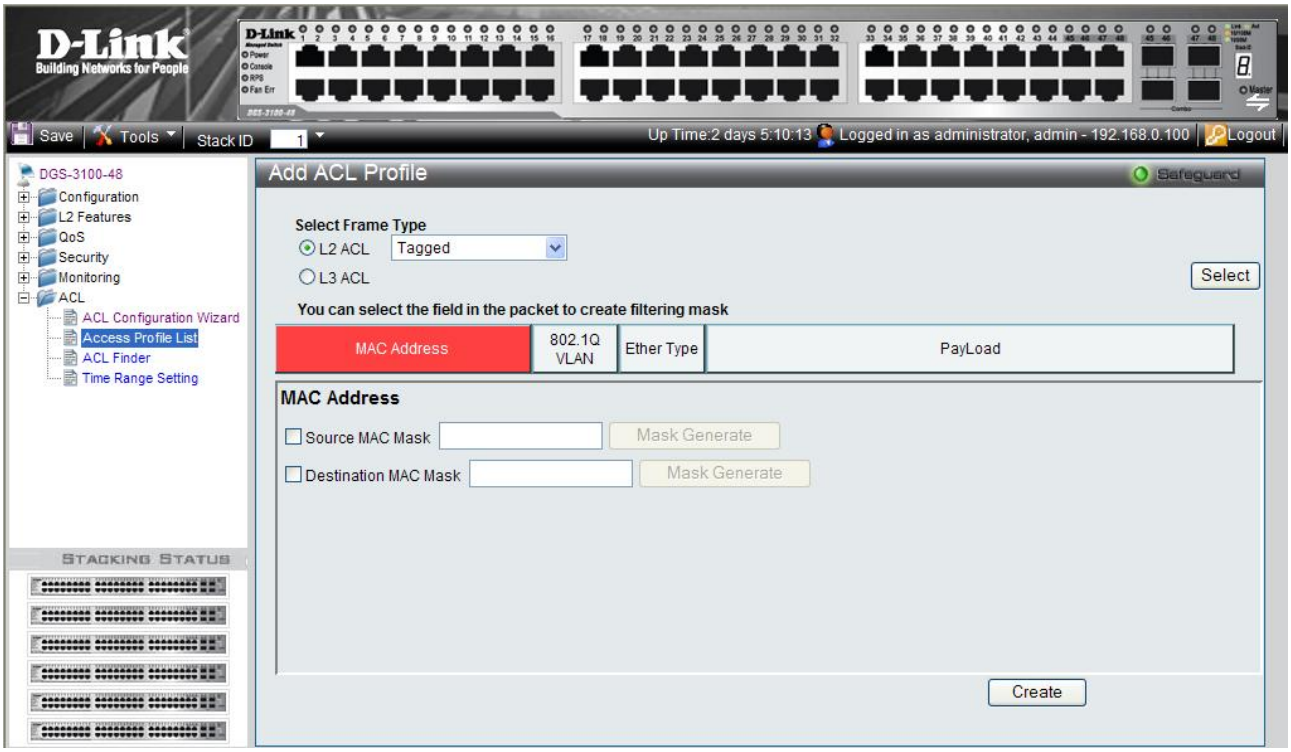


Figure 0-6 ACL Profile L2 ACL Tagged MAC Address Page

The ACL Profile L2 ACL Tagged MAC Address Page **contains the following fields:**

Field	Description
Source MAC Mask	Defines the range of source addresses relative to the ACL rules (0=ignore, 1=check). For example, to set 00:00:00:00:10:XX, use mask FF:FF:FF:FF:FF:00.
Destination MAC Mask	Defines the range of destination addresses relative to the ACL rules (0=ignore, 1=check). For example, to set 00:00:00:00:10:XX, use mask FF:FF:FF:FF:FF:00.

2. Select *Source MAC Mask* and/or *Destination MAC Mask*. The *Mask Generate* button is active.
3. Enter a MAC mask in the box adjacent to the *Mask Generate* button.

   Alternatively, click Mask Generate. The *Generate Mask by range* fields appear.

   Enter a MAC address range into the *Generate Mask by range* fields, and click Calculate. The mask is generated.
4. Click Create. The ACL profile is added, and the device is updated.

To define L2 802.1Q VLAN ACL profile:

1. Click the *802.1Q VLAN* button. The *ACL Profile L2 ACL Tagged VLAN Page* updates to show the following:

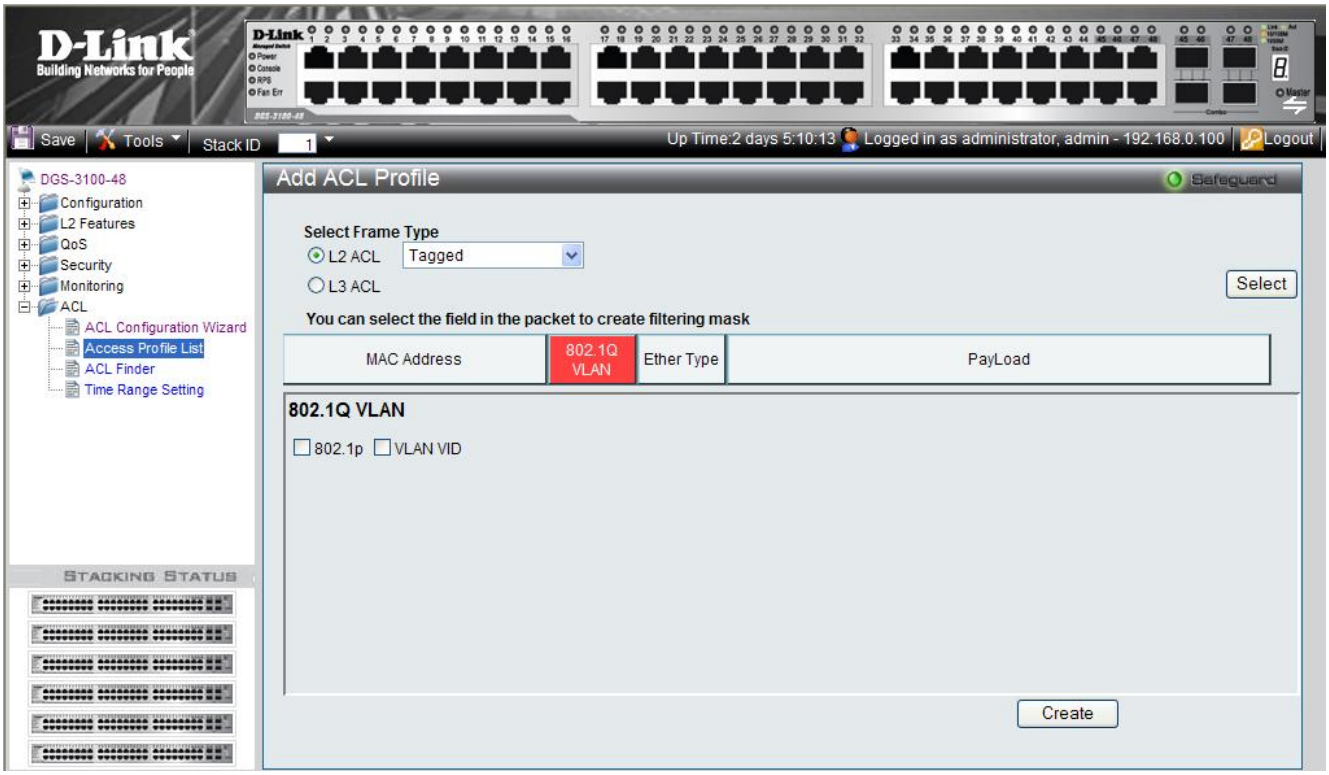


Figure 0-7 ACL Profile L2 ACL Tagged VLAN Page

The ACL Profile L2 ACL Tagged VLAN Page **contains the following fields:**

Field	Description
802.1p	Sets the 802.1p field as an essential field to match.
VLAN VID	Sets the VLAN VID field as an essential field to match.

2. Define the *802.1p* and *VLAN VID* fields.
3. Click Create. The ACL profile is added, and the device is updated.

To define L2 Ether Type ACL profile

This option defines whether or not the Ether Type field is checked for a match.

1. Click the Ether Type button. The *8 ACL Profile L2 ACL Tagged Ether Type* **Page** updates to show the following:

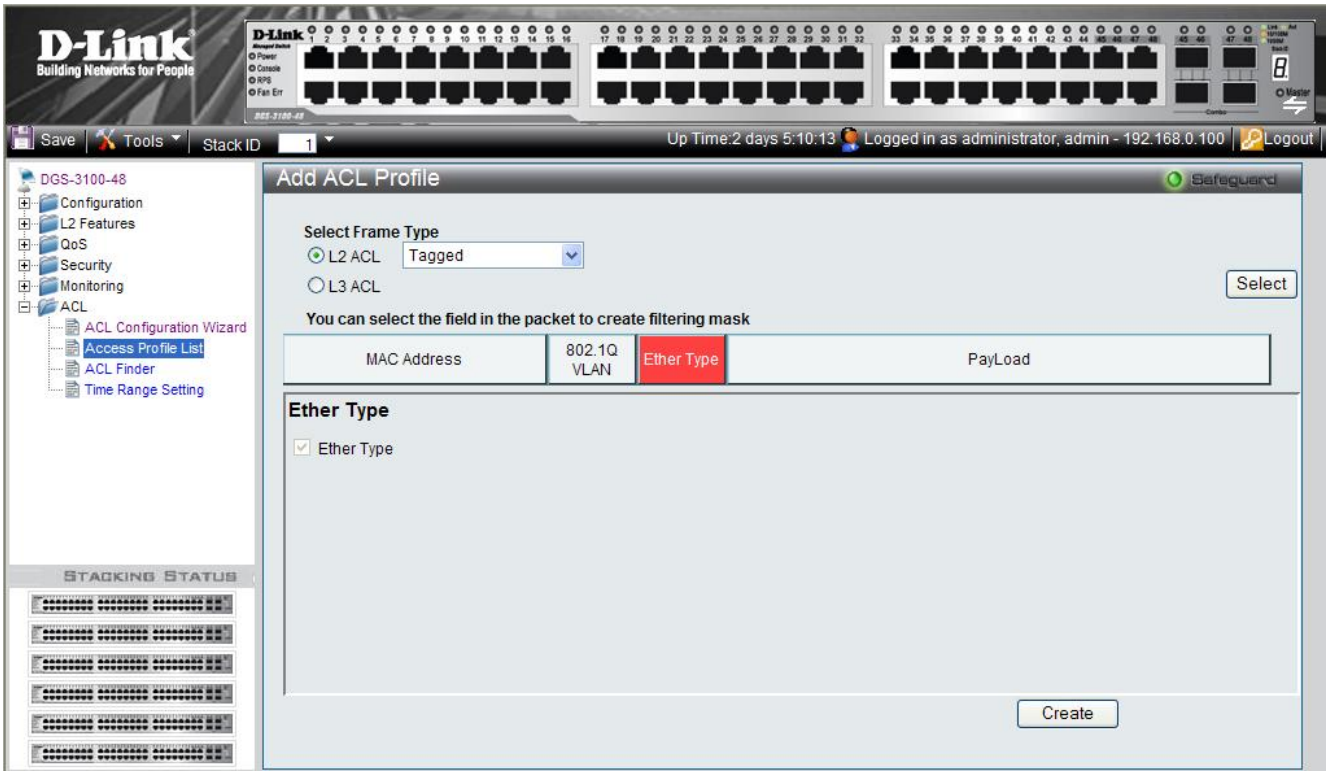


Figure 0-8 ACL Profile L2 ACL Tagged Ether Type Page

2. Click Create. The ACL profile is added, and the device is updated.

NOTE: A combination of one or several filtering masks can be selected simultaneously. The page updates with the relevant field(s).

Defining Layer 3 IPv4 ACL

Layer 3 IPv4 ACLs can be defined using the following filtering criteria:

- ICMP
- IGMP
- TCP
- UDP

The following sections describe each of these filtering options.

ICMP Filtering

To define ICMP filtering, select the ICMP option.

If *L3IPv4 ACL* *ICMP* is selected, the page updates as follows:

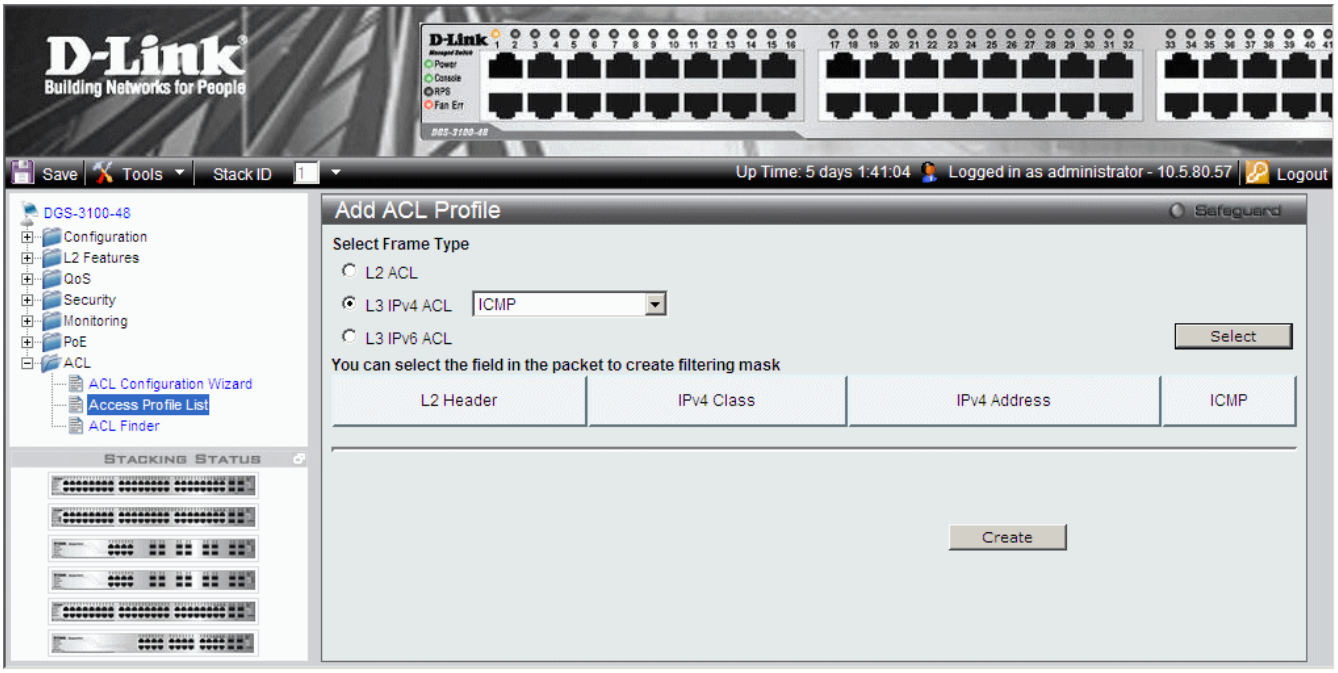


Figure 0-5 Add L3 IPv4 ACL Profile Page

The following sections describe how to select various ICMP filtering criteria for the ACLs

To define L3 IPv4 Class ACL profile:

This option defines whether or not the DSCP field is checked for a match.

1. Click the IPv4 Class button. The *ACL Profile L3 Ipv4 ACL ICMP Class Page* updates to show the following:

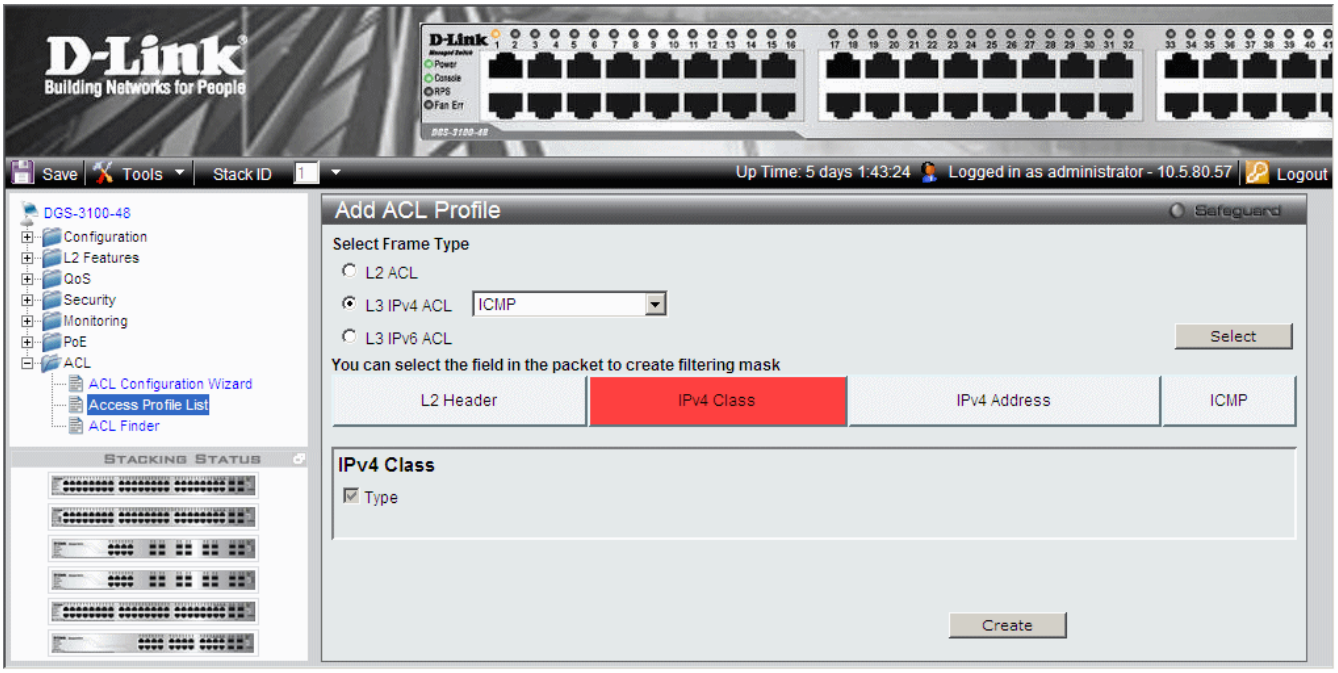


Figure 0-6 ACL Profile L3 Ipv4 ACL ICMP Class Page

2. Click Create. The ACL profile is added, and the device is updated.

To define L3 IPv4 Address ACL profile:

This option defines whether or not the address field is checked for a match.

1. Click the *IPv4 Address* button. The *ACL Profile L3 IPv4 ACL ICMP Address* **Page** updates to show the following:

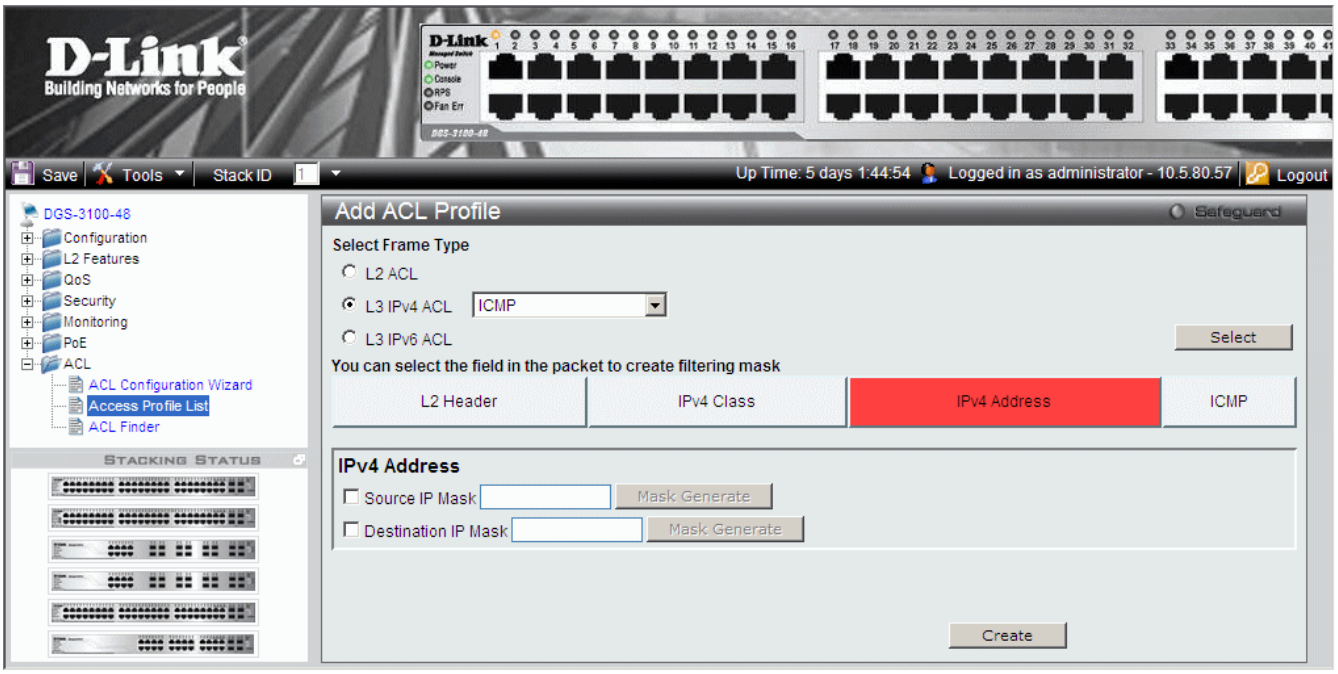


Figure 0-7 ACL Profile L3 IPv4 ACL ICMP Address Page

The ACL Profile L3 IPv4 ACL ICMP Address Page **contains the following fields:**

Field	Description
Source IP Mask	Defines the range of source IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0
Destination IP Mask	Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0

2. Select *Source IP Mask* and/or *Destination IP Mask*. The *Mask Generate* button is active.
3. Enter an IP mask in the box adjacent to the *Mask Generate* button.
4. Alternatively, click Mask Generate. The *Generate Mask by range* fields appear.
5. Enter an IP address range into the *Generate Mask by range* fields, and click Calculate. The mask is generated.
6. Click Create. The ACL profile is added, and the device is updated.

To define L3 IPv4 ICMP ACL profile:

1. Click ICMP. The *ACL Profile L3 IPv4 ACL ICMP Page* updates to show the following:

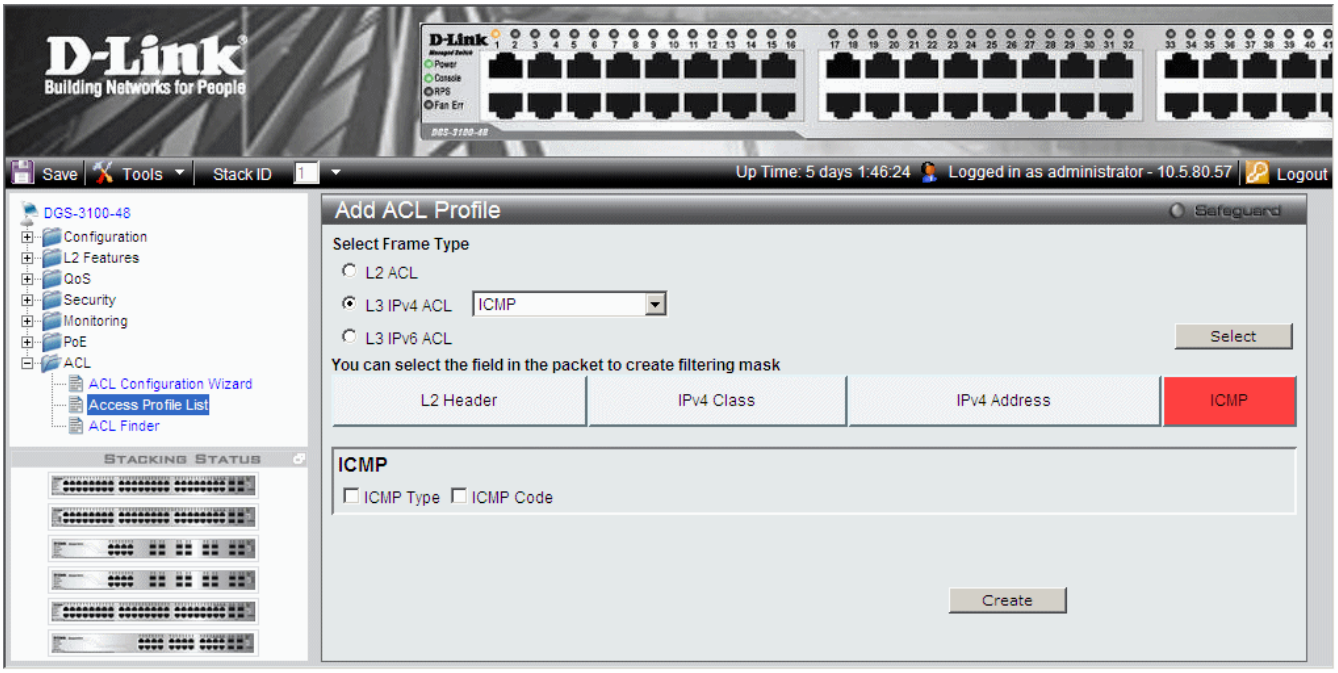


Figure 0-8 ACL Profile L3 IPv4 ACL ICMP Page

The ACL Profile L3 IPv4 ACL ICMP Page contains the following fields:

Field	Description
ICMP Type	Sets the ICMP Type field as an essential field to match.
ICMP Code	Sets the ICMP code field as an essential field to match.

2. Select the *ICMP Type* and/or *ICMP Code* fields.
3. Click Create. The ACL profile is added, and the device is updated.

IGMP Filtering

To define IGMP filtering, select the IGMP option.

To define L3 IPv4 IGMP ACL profile:

1. Select IGMP. The ***ACL Profile L3 IPv4 IGMP Page*** updates as follows:

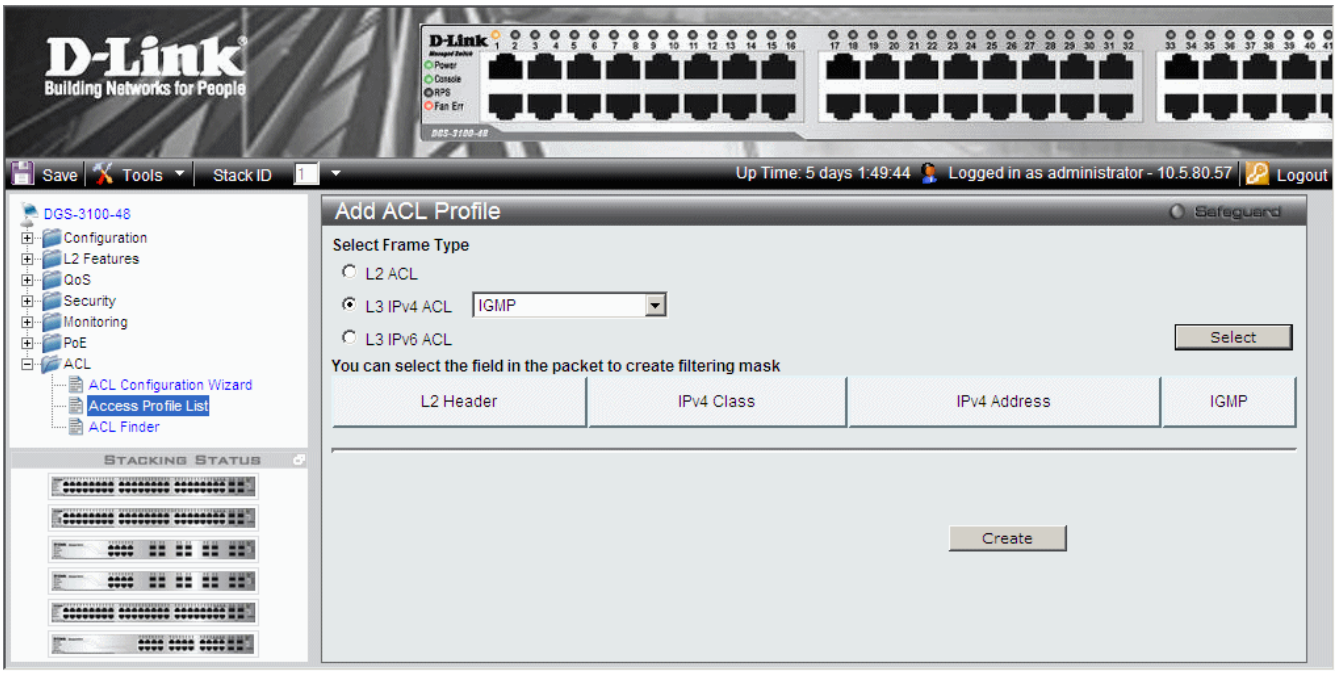


Figure 0-9 ACL Profile L3 IPv4 IGMP Page

2. Click the IGMP button. The ACL Profile L3 IPv4 IGMP Selected **Page** updates to show the following:

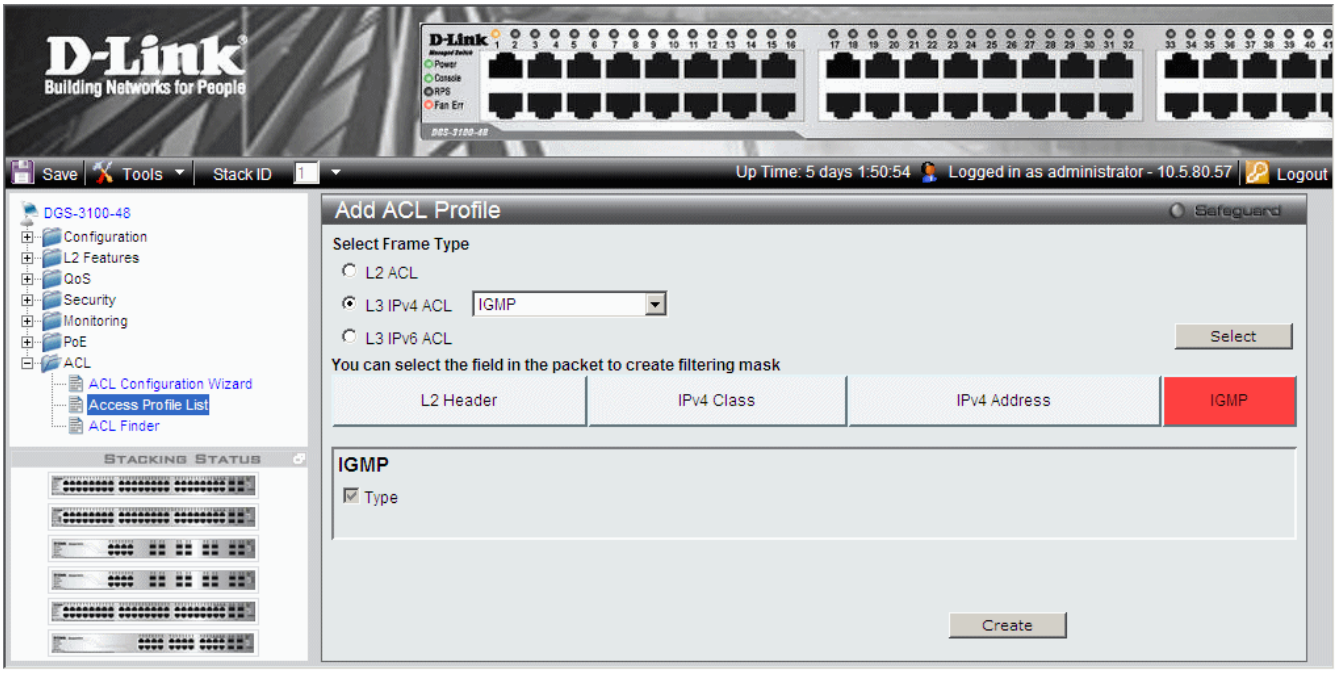


Figure 0-10 ACL Profile L3 IPv4 IGMP Selected Page

3. Click Create. The ACL profile is added, and the device is updated.

TCP Filtering

To define TCP filtering, select the TCP option.

If *L3 IPv4 ACL* *TCP* is selected, the page updates as follows:

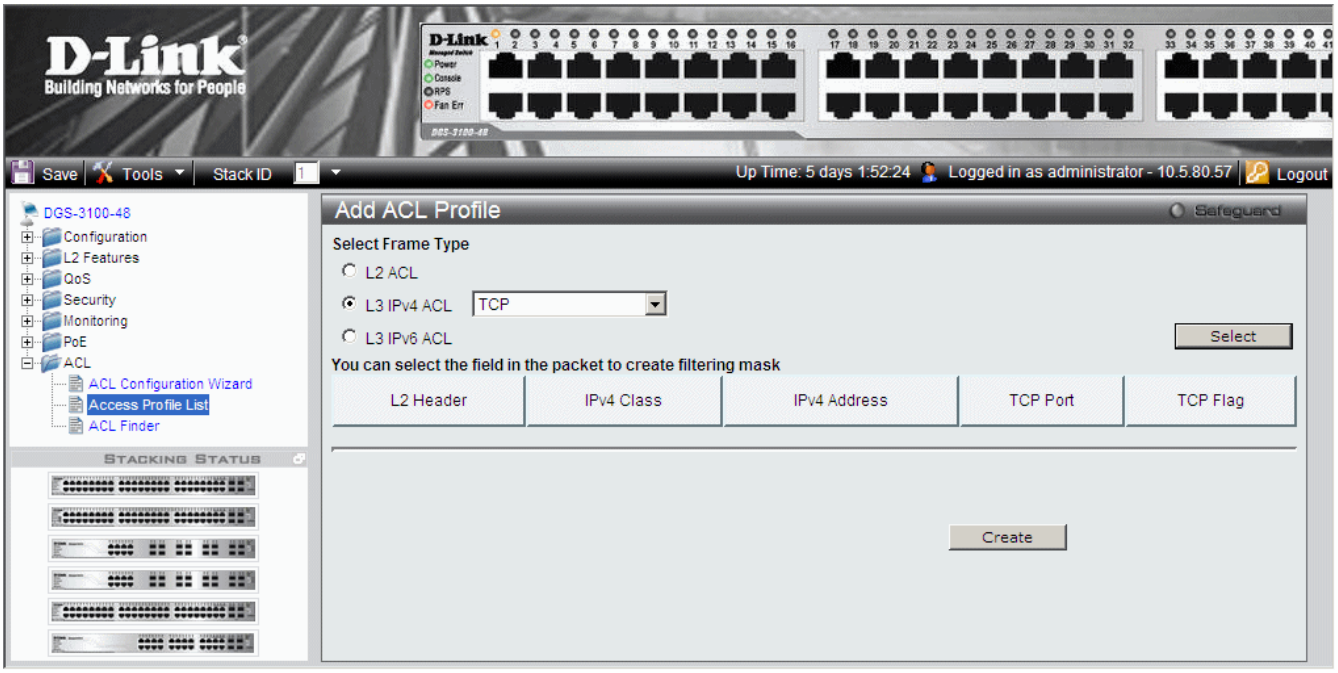


Figure 0-11 ACL Profile L3 IPv4 TCP Page

To define L3 IPv4 TCP Port ACL profile:

1. Click the TCP Port button. The *ACL Profile L3 Ipv4 TCP Port Page* updates to show the following:

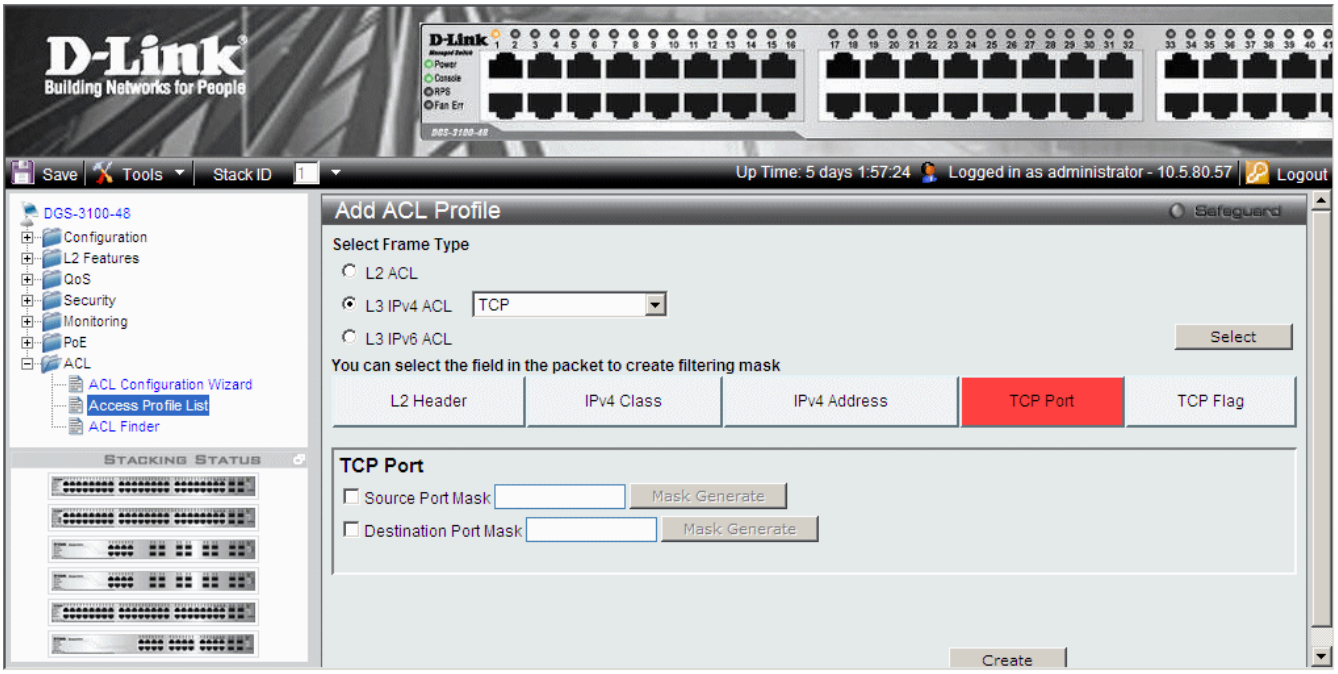


Figure 0-12 ACL Profile L3 Ipv4 TCP Port Page

The ACL Profile L3 Ipv4 TCP Port Page contains the following fields:

Field	Description
Source Port Mask	Defines the range of source Ports relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.
Destination Port Mask	Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.

2. Select *Source Port Mask* and/or *Destination Port Mask*. The *Mask Generate* button is active.

3. Enter a port ID in the box adjacent to the *Mask Generate* button.
4. Alternatively, click Mask Generate. The *Generate Mask by range* fields appear.
5. Enter a port ID range into the *Generate Mask by range* fields, and click Calculate. The mask is generated.
6. Click Create. The ACL profile is added, and the device is updated.

To define L3 IPv4 TCP Flag ACL Profile:

This option defines whether or not the TCP Flag field is checked for a match.

1. Click the *TCP Flag* button. The *ACL Profile L3 Ipv4 TCP Flag Page* updates to show the following:

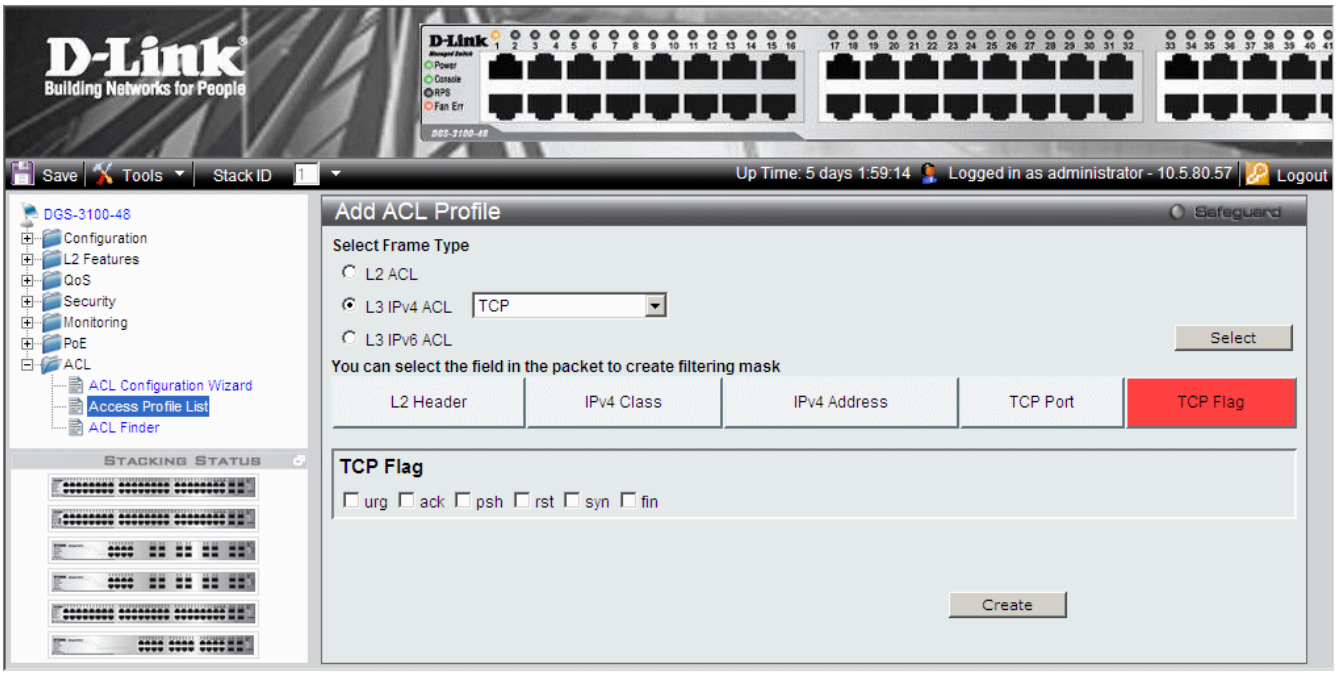


Figure 0-13 ACL Profile L3 Ipv4 TCP Flag Page

2. Click Create. The ACL profile is added, and the device is updated.

UDP Filtering

To define UDP filtering, select the UDP option.

If *L3 IPv4 ACL* *UDP* is selected, the page updates as follows:

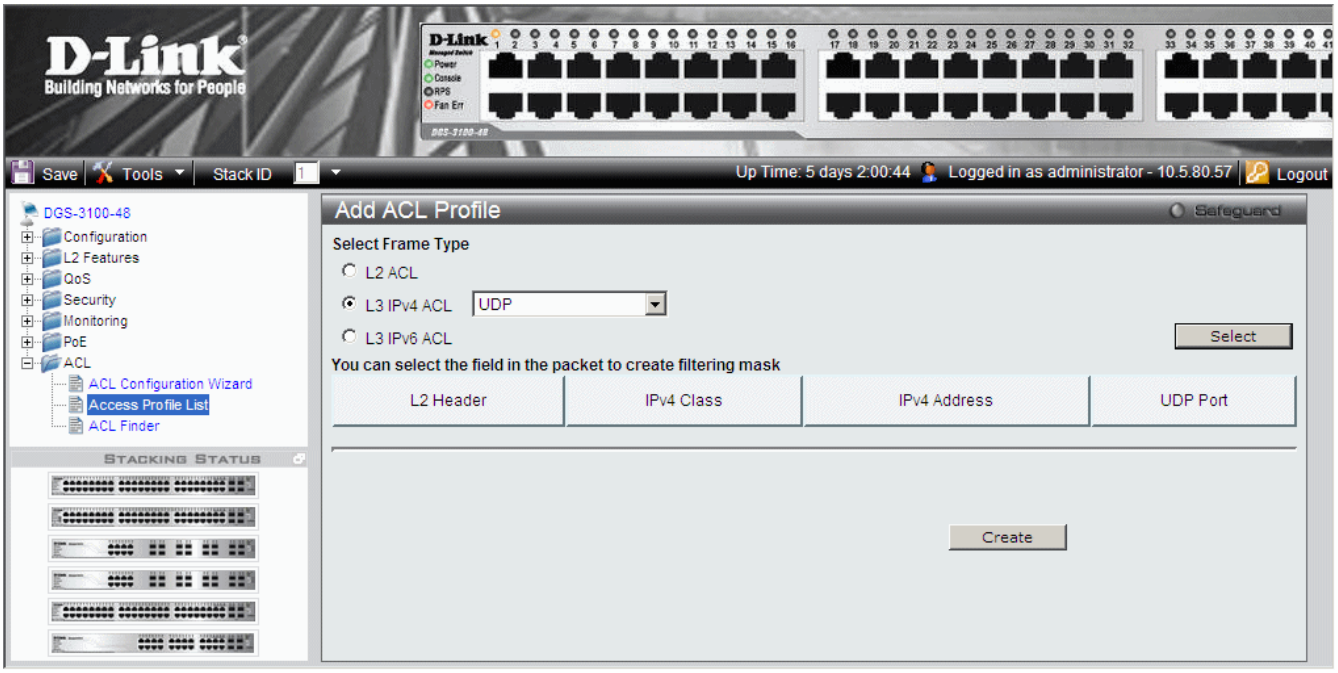


Figure 0-14 ACL Profile L3 IPv4 UDP Page

To define L3 IPv4 UDP Port ACL profile:

1. Click the UDP Port button. The *ACL Profile L3 IPv4 UDP Port Page* updates to show the following:

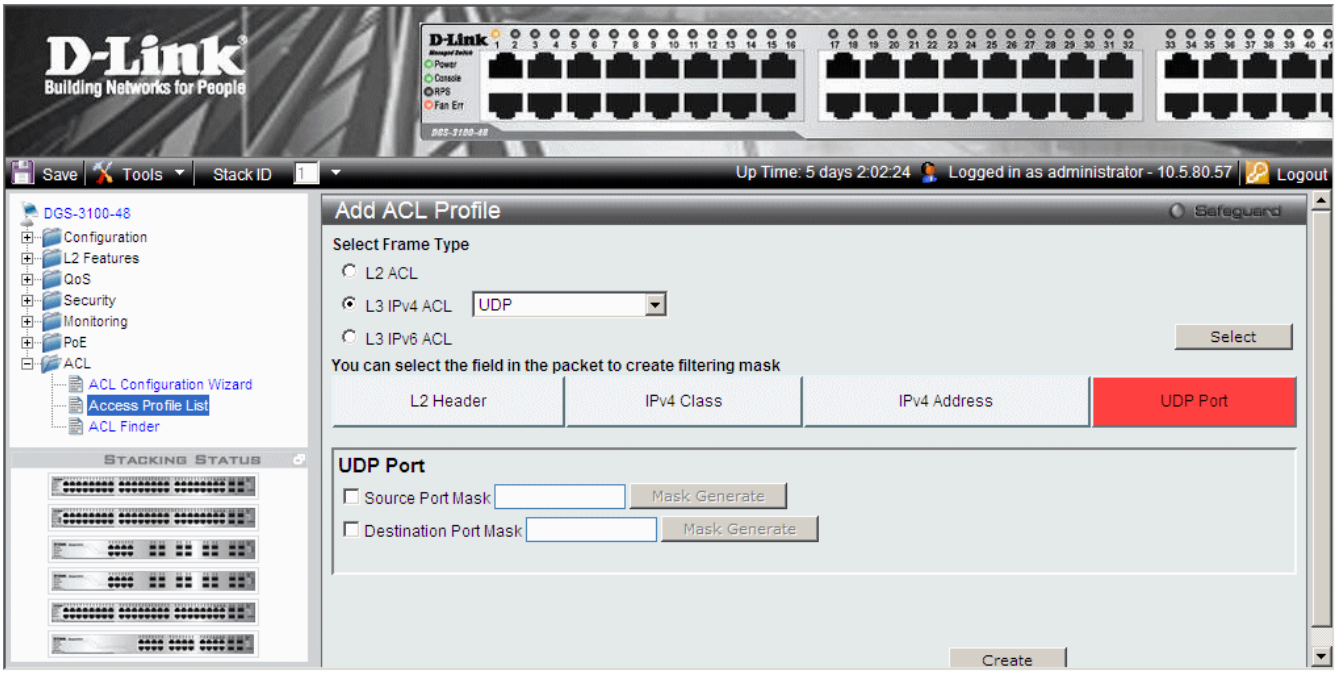


Figure 0-15 ACL Profile L3 IPv4 UDP Port Page

The ACL Profile L3 IPv4 UDP Port Page contains the following fields:

Field	Description
Source Port Mask	Defines the range of source Ports relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of F.
Destination Port Mask	Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of F.

2. Select *Source Port Mask* and/or *Destination Port Mask*. The *Mask Generate* button is active.

3. Enter a port ID in the box adjacent to the *Mask Generate* button.
4. Alternatively, click Mask Generate. The *Generate Mask by range* fields appear.
5. Enter a port ID range into the *Generate Mask by range* fields, and click Calculate. The mask is generated.
6. Click Create. The ACL profile is added, and the device is updated.

NOTE: A combination of one or several filtering masks can be selected simultaneously. The page updates with the relevant field(s).

Defining Layer 3 IPv6 ACL

Layer 3 IPv6 ACLs can be defined using the following filtering criteria:

- ICMP
- TCP
- UDP

The following sections describe each of these filtering options.

ICMP Filtering

If *L3 IPv6 ACL* *ICMP* is selected, the page updates as follows:

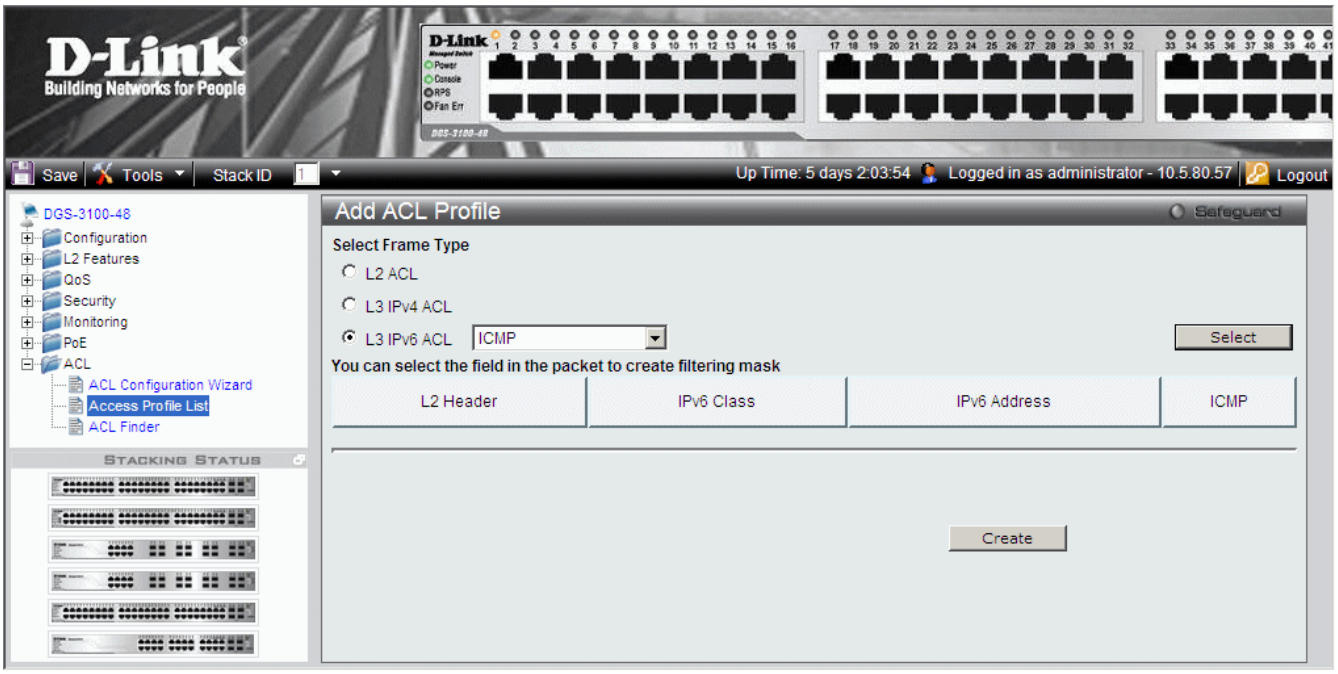


Figure 0-16 Add L3 IPv6 ACL Profile Page

To define L3 IPv6 Class ACL profile:

This option defines whether or not the Class field is checked for a match.

1. Click the IPv6 Class button. The *ACL Profile L3 Ipv4 ACL ICMP Class Page* updates to show the following:

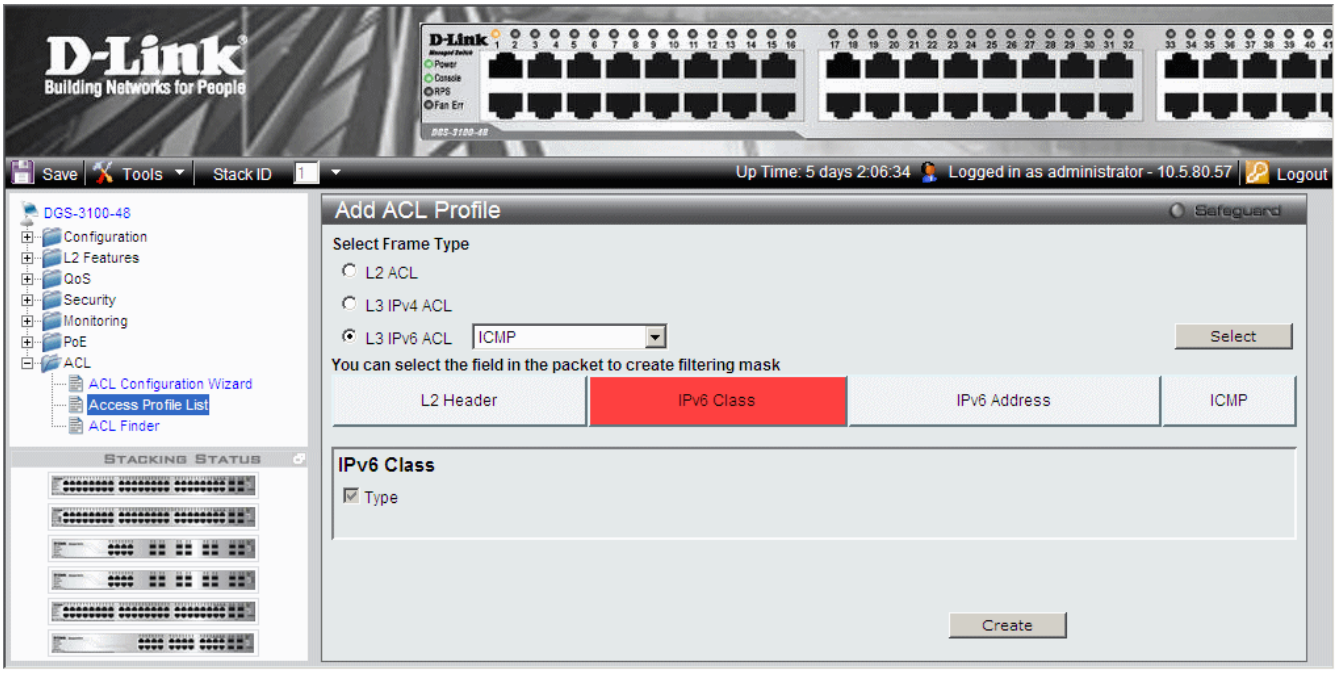


Figure 0-17 ACL Profile L3 IPv6 ACL ICMP Class Page

2. Click Create. The ACL profile is added, and the device is updated.

To define L3 IPv6 Address ACL profile:

1. Click the *IPv6 Address* button. The *ACL Profile L3 IPv4 ACL ICMP Address* **Page** updates to show the following:

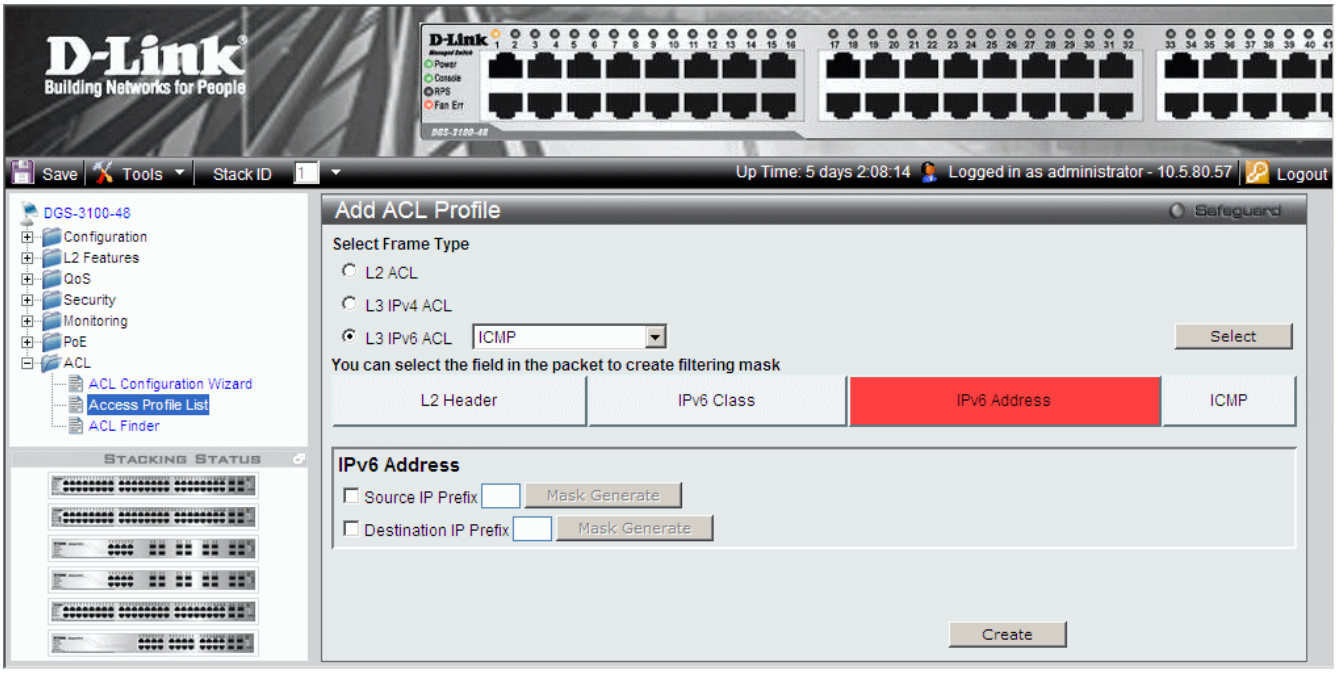


Figure 0-18 ACL Profile L3 IPv6 ACL ICMP Address Page

The ACL Profile L3 IPv4 ACL ICMP Address Page **contains the following fields:**

Field	Description
Source IP Prefix	Defines the range of source IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 2002:0:0:0:0:0:b0d4:0, use mask 128
Destination IP Prefix	Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore,

Field	Description
	1=check). For example, to set 2002:0:0:0:0:0:bfd4:0, use mask 128

2. Select *Source IP Mask* and/or *Destination IP Mask*. The *Mask Generate* button is active.
3. Enter an IP mask in the box adjacent to the *Mask Generate* button.
4. Alternatively, click Mask Generate. The *Generate Mask by range* fields appear.
5. Enter an IP address range into the *Generate Mask by range* fields, and click Calculate. The mask is generated.
6. Click Create. The ACL profile is added, and the device is updated.

To define L3 IPv6 ICMP ACL profile:

1. Click the ICMP button. The *ACL Profile L3 IPv4 ACL ICMP Page* updates to show the following:

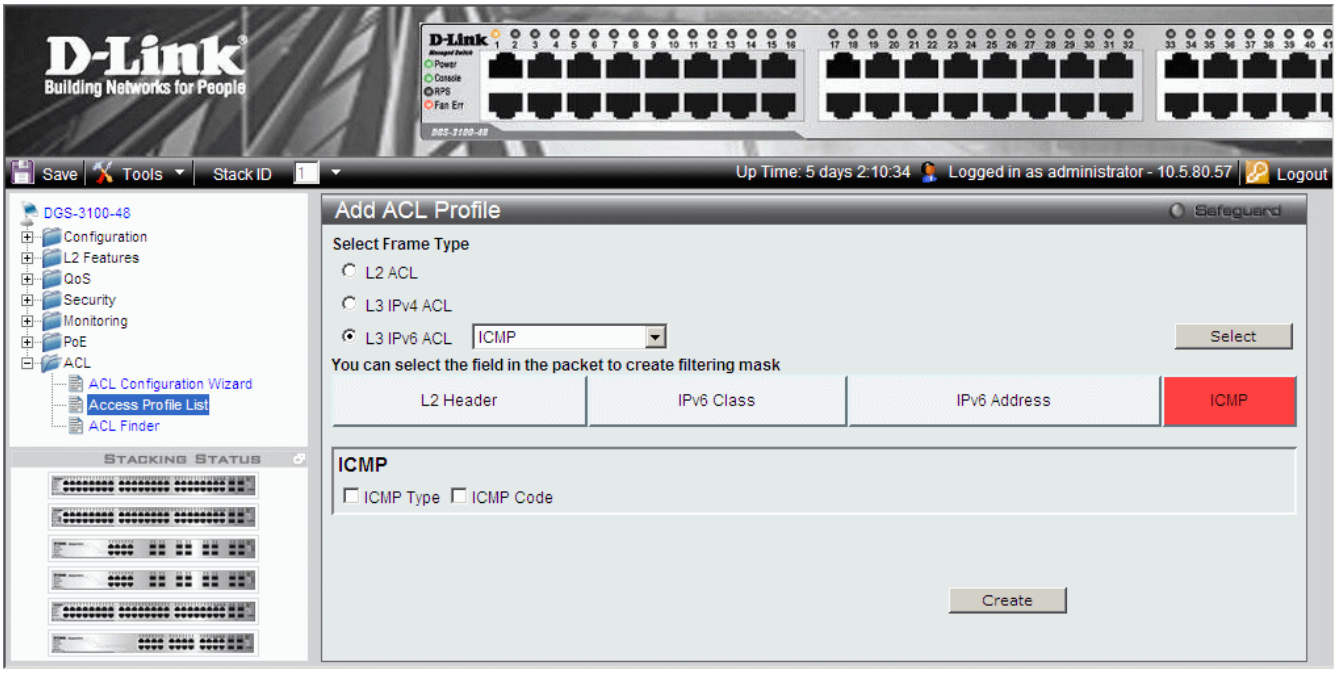


Figure 0-19 ACL Profile L3 IPv6 ACL ICMP Page

The ACL Profile L3 IPv4 ACL ICMP Page contains the following fields:

Field	Description
ICMP Type	Sets the ICMP Type field as an essential field to match.
ICMP Code	Sets the ICMP code field as an essential field to match.

2. Select the *ICMP Type* and/or *ICMP Code* fields.
3. Click Create. The ACL profile is added, and the device is updated.

TCP Filtering

If *L3 IPv6 ACL TCP* is selected, the page updates as follows:

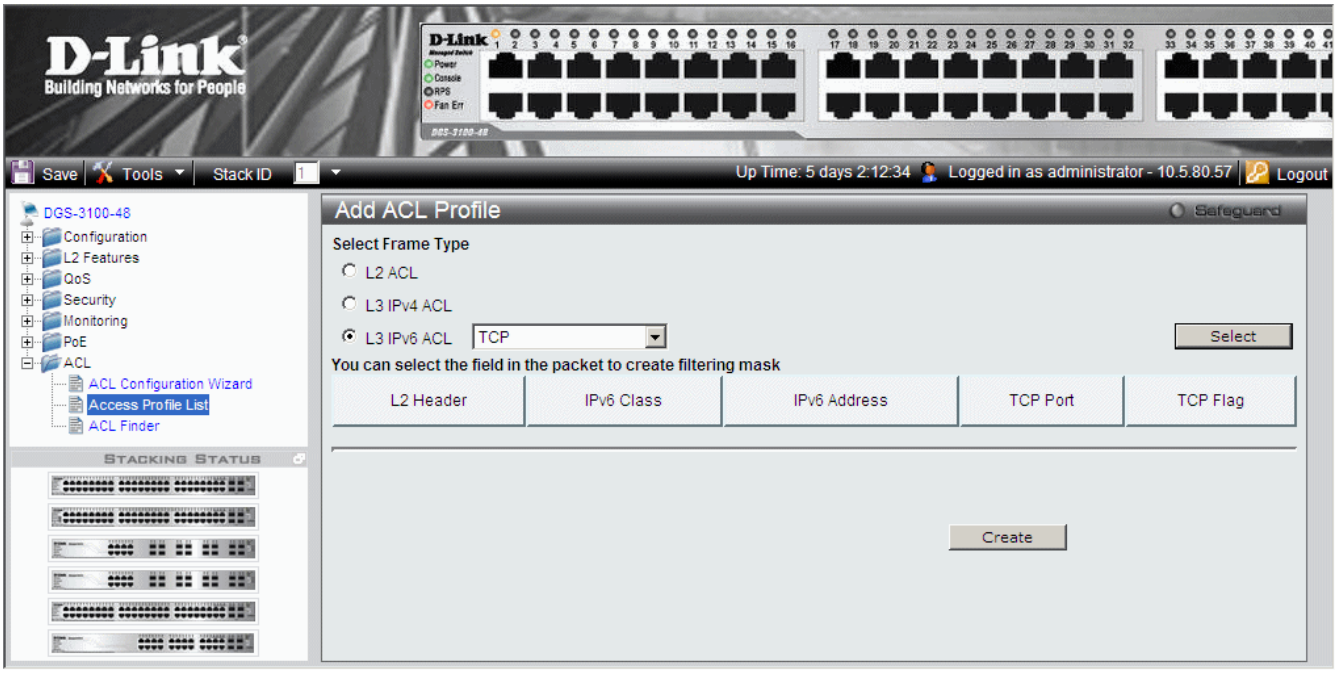


Figure 0-20 ACL Profile L3 IPv6 TCP Page

To define L3 IPv6 TCP Port ACL profile:

1. Click the TCP Port button. The *ACL Profile L3 Ipv4 TCP Port Page* updates to show the following:

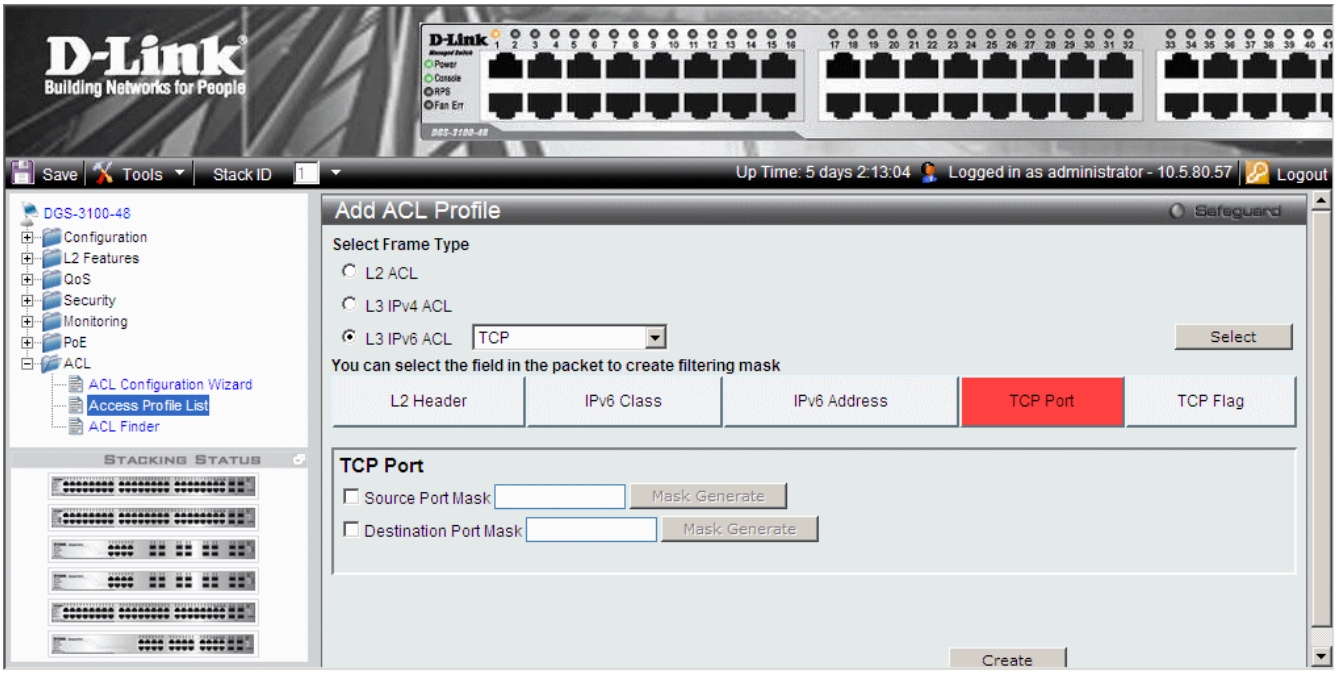


Figure 0-21 ACL Profile L3 IPv6 TCP Port Page

The ACL Profile L3 Ipv4 TCP Port Page contains the following fields:

Field	Description
Source Port Mask	Defines the range of source Ports relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.
Destination Port Mask	Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.

2. Select *Source Port Mask* and/or *Destination Port Mask*. The *Mask Generate* button is active**.**

3. Enter a port ID in the box adjacent to the *Mask Generate* button.
4. Alternatively, click Mask Generate. The *Generate Mask by range* fields appear.
5. Enter a port ID range into the *Generate Mask by range* fields, and click Calculate. The mask is generated.
6. Click Create. The ACL profile is added, and the device is updated.

To define L3 IPv6TCP Flag ACL Profile:

This option defines whether or not the TCP Flag field is checked for a match.

1. Click the *TCP Flag* button. The *ACL Profile L3 Ipv4 TCP Flag Page* updates to show the following:

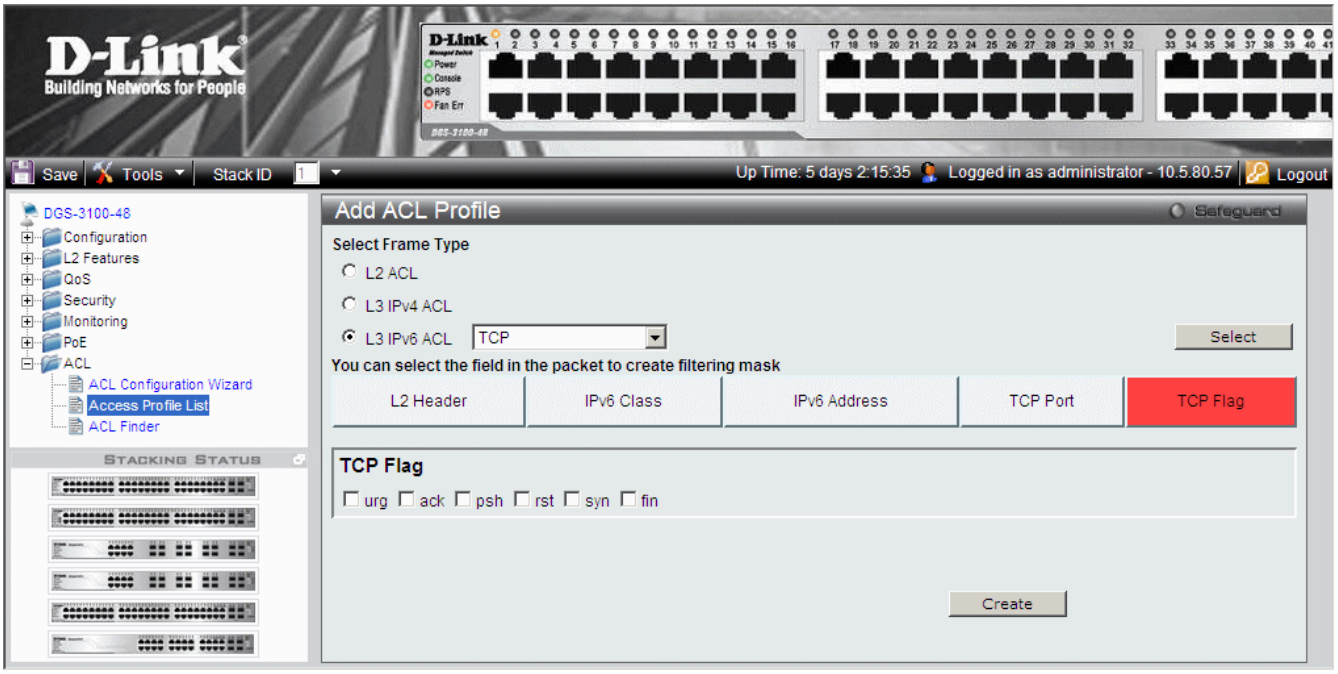


Figure 0-22 ACL Profile L3 IPv6 TCP Flag Page

2. Click Create. The ACL profile is added, and the device is updated.

UDP Filtering

If L3 IPv6 ACL UDP is selected, the page updates as follows:

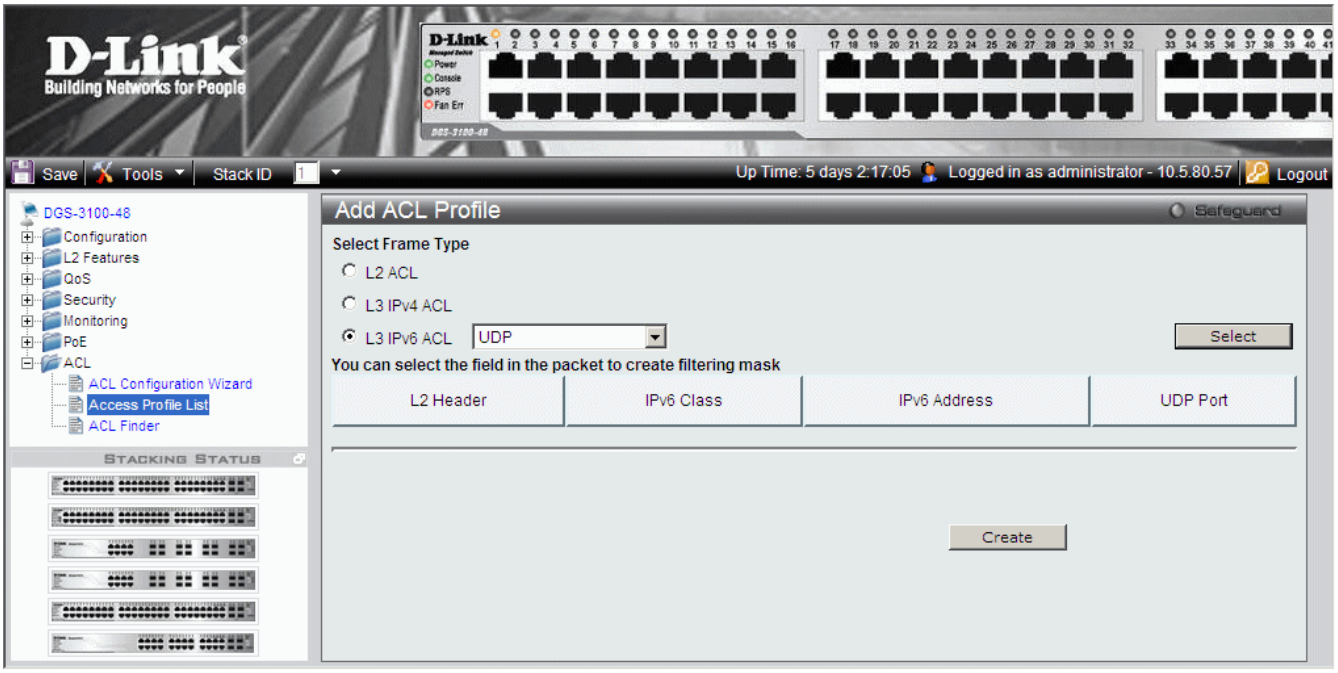


Figure 0-23 ACL Profile L3 IPv6 UDP Page

To define L3 IPv6 UDP Port ACL profile:

1. Click the UDP Port button. The *ACL Profile L3 IPv4 UDP Port Page* updates to show the following**:**

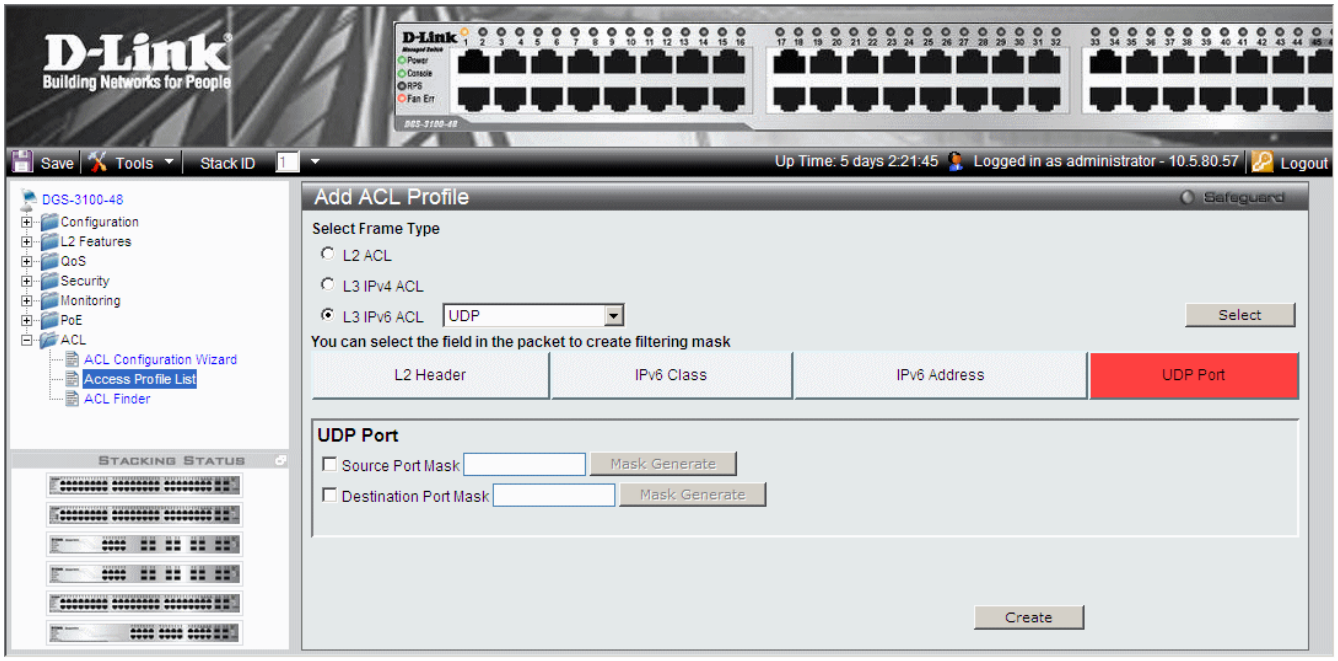


Figure 0-24 ACL Profile L3 IPv6 UDP Port Page

The ACL Profile L3 IPv4 UDP Port Page contains the following fields:

Field	Description
Source Port Mask	Defines the range of source Ports relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of F.
Destination Port Mask	Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of F.

2. Select *Source Port Mask* and/or *Destination Port Mask*. The *Mask Generate* button is active**.**

3. Enter a port ID in the box adjacent to the *Mask Generate* button.
4. Alternatively, click Mask Generate. The *Generate Mask by range* fields appear.
5. Enter a port ID range into the *Generate Mask by range* fields, and click Calculate. The mask is generated.
6. Click Create. The ACL profile is added, and the device is updated.

NOTE: A combination of one or several filtering masks can be selected simultaneously. The page updates with the relevant field(s).

IP and MAC-Based ACLs on the Same Port

IPv6-based ACLs and MAC-based ACLs cannot be defined on the same port. The user can, however, set IPv4-based ACL and MAC-based ACL on the same port(s). This is performed in the following: way:

- Go to 'Add Access Profile' page.
- Add L2 Access Profile with the desired fields.
- Add L3 IPv4-based Access Profile with the desired fields.
- Go to 'Access Rule List' page, create rules for both profiles and apply it on the same port(s) /LAG(s).

Now you have both an IPv4-based ACL and MAC-based ACL on the port(s) /LAG(s).

NOTE**:** Adding rules to specific profile generates a unique Access ID in the range 1-240.
When the user adds a rule to different profiles he cannot use the same Access ID for different rules.

Adding Access Rules

The following conditions can be defined as Access Rules:

Filter	Description
Source Port IP Address and Wildcard Mask	Filters the packets by the Source port IP address and wildcard mask.
Destination Port IP Address and Wildcard Mask	Filters the packets by the Source port IP address and wildcard mask.
Protocol	Filters the packets by the Layer 4 protocol.
DSCP	Filters the packets by the DiffServ Code Point (DSCP) value.
Class	Filters the packets by the Class value.
IP Precedence	Filters the packets by the IP Precedence.
Action	Indicates the action assigned to the packet matching the ACL conditions. Packets are forwarded, dropped or going through QoS action.

To add/change an access rule:

1. Click **ACL > Access Profile List**: The *Access Profile List Page* opens**.**

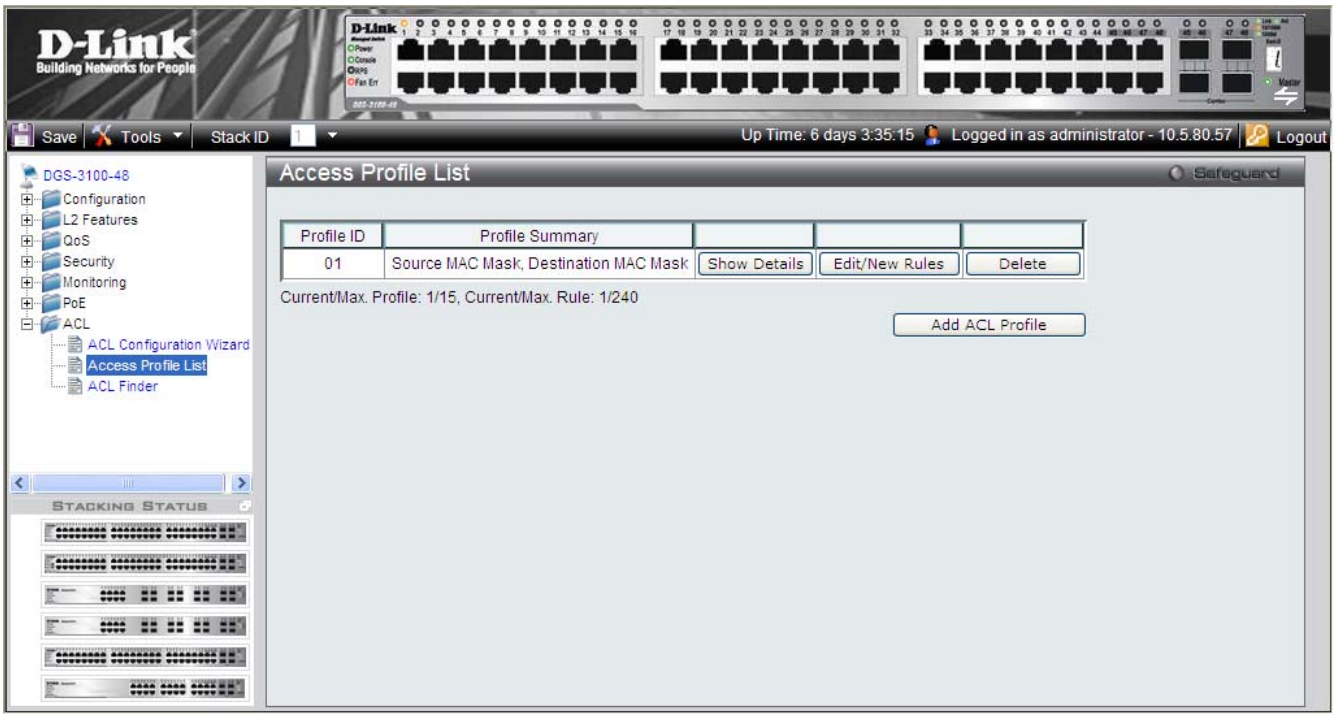


Figure 0-25 Access Profile List Page

1. Select a profile and click Edit/New Rules. The Access Rule List Page opens:

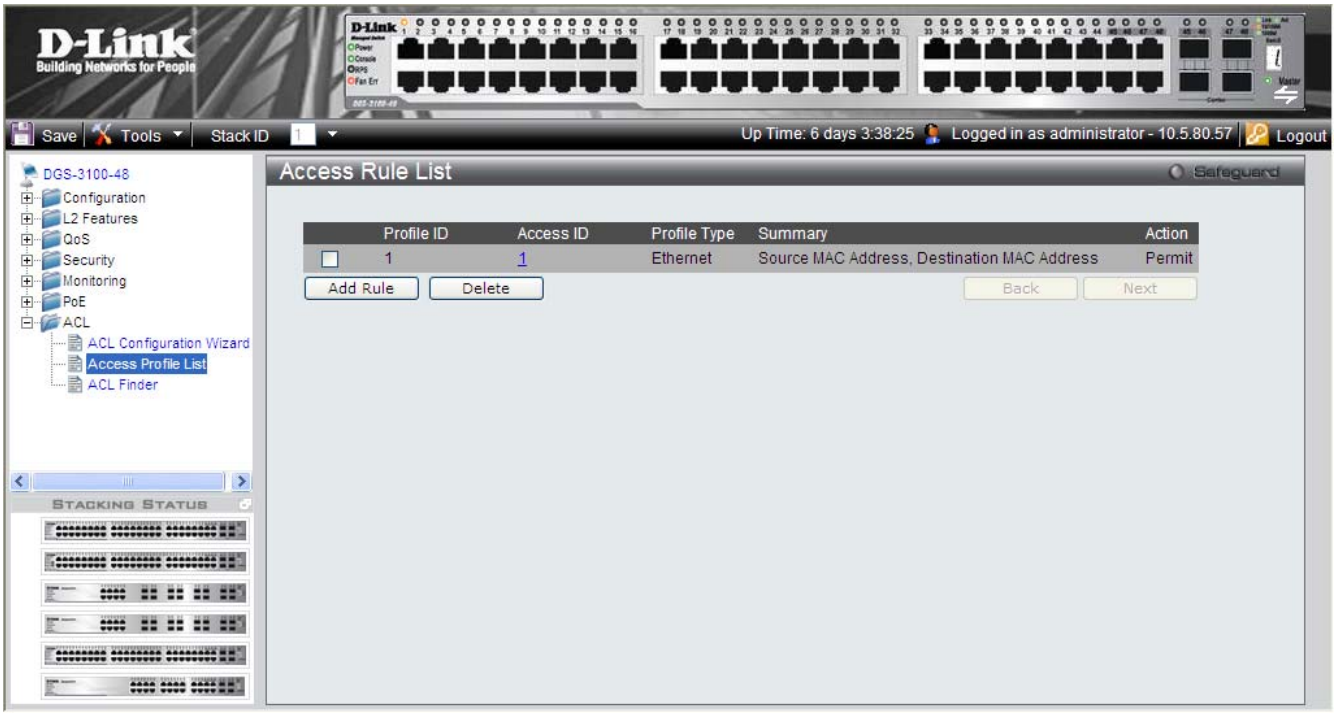
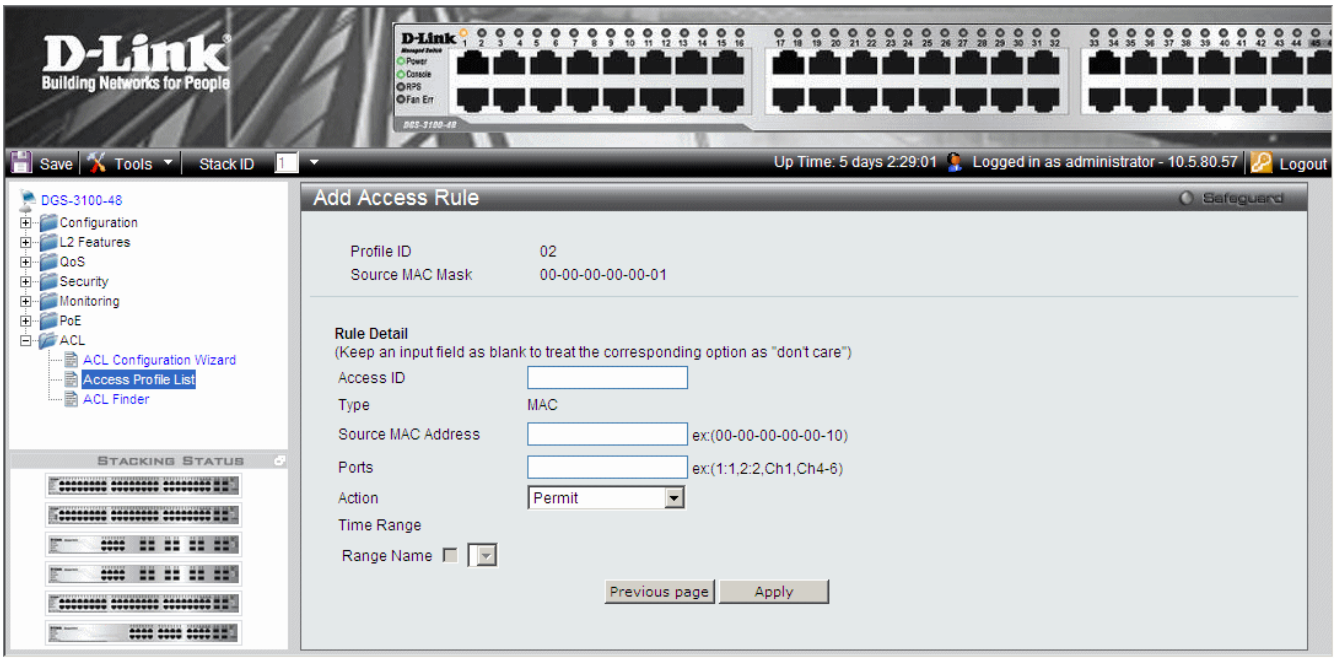


Figure 0-26 Add Access Rule Page (IP based ACL)

2. Click Add Rule. The Add Access Rule Page opens. The fields in this page depend on the type of ACL to which a rule is being added. The page below is displayed for a MAC-Address ACL.



This page displays all or some of the following fields:

Field	Description
Profile ID	Displays the Profile ID to which the rule is being added to.
Source MAC/IPv4/IPv6 Mask	Displays the MASK defined in the Profile
Destination MAC/IPv4/IPv6 Mask	Displays the MASK defined in the Profile
Source MAC/IPv4/IPv6 Address	Defines the address on which the rule is defined.
Destination MAC/IPv4/IPv6 Address	Defines the address on which the rule is defined.
TCP Source Port	Displays The TCP Source Port.
TCP Flag Mask	Indicates if TCP flag mask is active.
Access ID	Defines the Access ID
Type	Displays the profile type (IP based).
TCP Flag	Defines the indicated TCP flag that can be triggered.
Source Port	Displays the TCP source port.
Ports	Defines the ports or LAGs on which the access profile will work.
Action	Defines the action to be taken The possible values are: • Permit — Forwards packets if all other ACL criteria are met. • Deny — Drops packets if all other ACL criteria is met. • Rate Limiting — Rate limiting is activated if all other ACL criteria are met. • Change 1P priority — VPT (CoS) value is changed if all other ACL criteria is met. • Replace DSCP — Reassigns a new DSCP value to the packet if all other ACL criteria are met.

Field	Description
Time Range	Specifies whether the access rule is time-based.
Range Name	Selects the user-defined time range name to apply to the access rule.

3. Define the *Rule Detail* fields.
4. Click Apply. The rule is changed, and the device is updated.

NOTE: Each Access Profile must create rules with unique Access IDs. Access IDs cannot overlap in two different Access Profiles.

Finding ACL Rules

The *ACL Finder Page* identifies any rule which has been assigned to a specific port. To find ACL rules:

1. Click **ACL > ACL Finder**: The *ACL Finder Page* opens:

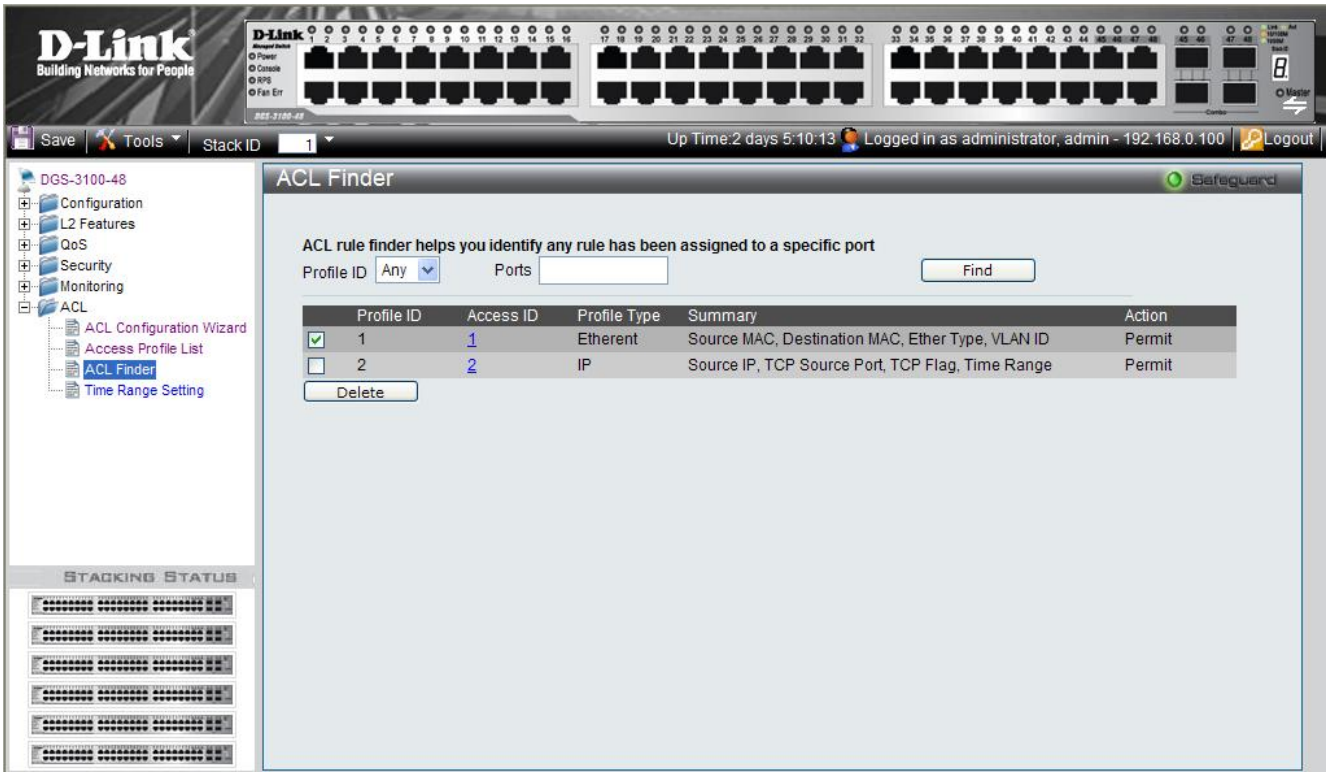


Figure 0-31 ACL Finder Page

The ACL Finder Page contains the following fields:

Field	Description
Profile ID (list box)	Defines the Profile ID for the search
Ports	Indicates the ports or LAGs for which rules are sought
Profile ID	Indicates the Profile ID
Access ID	Indicates the ACL rule ID number.
Profile Type	Indicates if the profile is IP or Ethernet
Summary	Displays the access rule.
Action	Displays the action chosen for the profile.

2. Define the *Profile ID* and *Ports* fields.
3. Click Find. The ACL rule is displayed**.**

To delete an ACL Profile entry:

1. Select the entry.
2. Click Delete. The entry is deleted.
3. Click OK. The entry is deleted**.**

To view or define the rule details:

1. Click the Access ID (linked number). The Rule Detail Page opens**:**

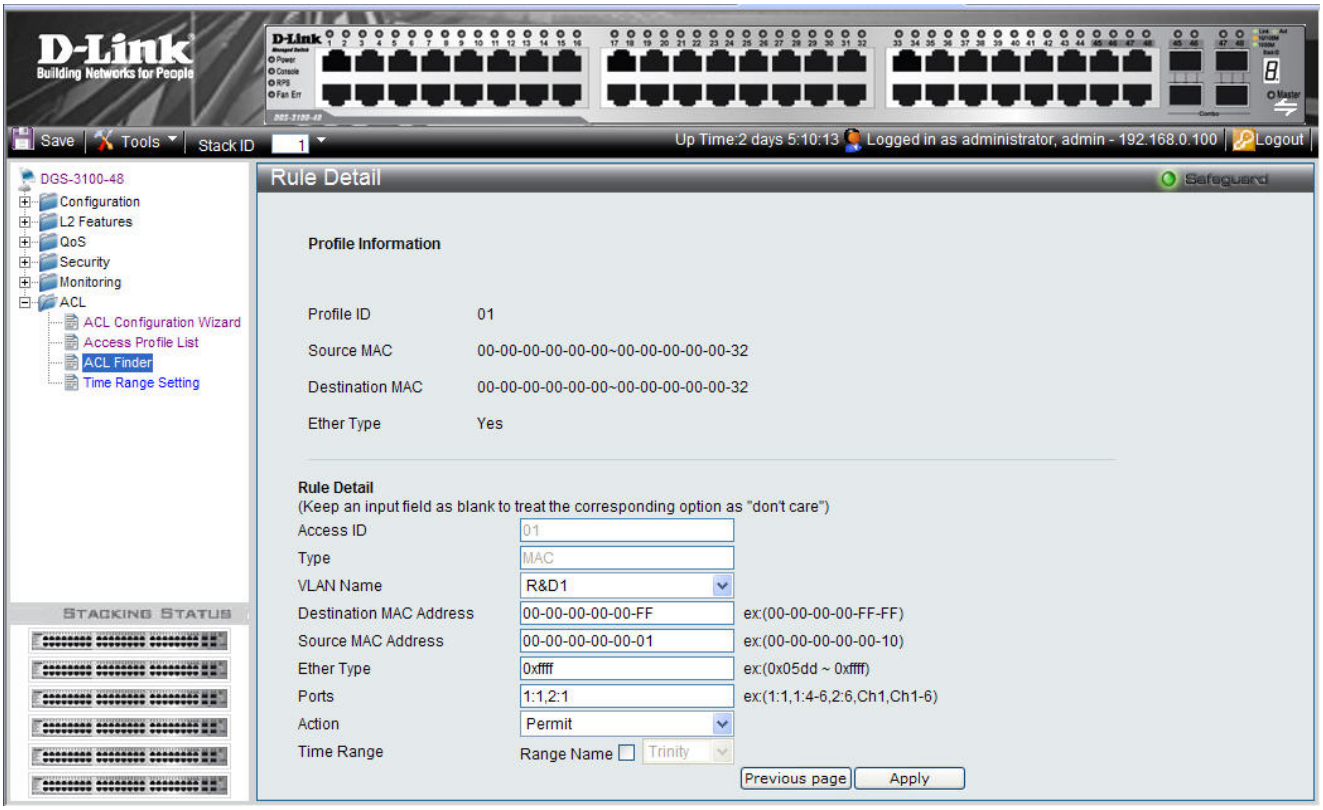


Figure 0-32 Rule Detail Page

The Rule Detail Page contains the following fields:

Field	Description
Profile ID	Displays the profile ID range.
Source MAC	Displays the Source MAC range.
Destination MAC	Displays the destination MAC range.
Ether Type	Displays if Ether Type is included.
Access ID	Defines the Access ID
Type	Displays the profile type (can be MAC based or IP based).
VLAN Name	Defines the user-defined VLAN name.
Destination MAC Address	Matches the destination MAC address to which packets will be subject to action.
Source MAC Address	Matches the source MAC address to which packets will be subject to action.
Ether Type	Defines the code type used.
Ports	Indicates the ports or LAGs for which rules are sought.
Action	Defines the action for the profile. The possible fields are: *Permit* — Forwards packets if all other ACL criteria are met. *Deny* — Drops packets if all other ACL criteria is met. *Rate Limiting* — Rate limiting is activated if all other ACL criteria are met. *Change 1P priority* — VPT (CoS) value is changed if all other ACL criteria is met. *Replace DSCP* — Reassigns a new DSCP value to the packet if all other ACL criteria are met.
Time Range	Specifies whether the access rule is time-based.
Range Name	Selects the user-defined time range name to apply to the access rule.

2. Define the *Rule Detail* fields.
3. Click Apply. The rule is defined, and the device is update

Notes about ACLs capacity in the DGS-3100 Series

- The user can create up to 15 Access Profiles.
- The user can configure up to 240 Access IDs, each Access ID is unique i.e. the same Access ID can't be created from two different Access Profiles.
- The maximum capacity of DGS-3100 series is 240 rules.
- The rules count will be done according to the following guidelines:
- The user should accumulate the rules of every unique set of rules (a unique set of rules is the same set of rules which is bound to one or more than one ports) /LAG(s)..
- The outcome of the above is that Access ID will be counted as a rule 'n' times where 'n' is the number of different settings of rules on different ports /LAG(s)..

- Examples for capacity calculations:
- Example #1:
  - Assume that Access IDs 1, 2, 3, 4 are bound to ports: 1-30, this is a unique set of rules and the count of rules in this case is 4.
  - Assume that Access IDs 5, 6 are bound to ports: 31-40, this is another unique set of rules and the count of additional rules will be 2.
  - Totally in the system we will use 6 rules out of the available 240!

- Example #2:
  - Assume that Access IDs 1, 2, 3, 4 are bound to ports: 1-10, this is a unique set of rules and the count of rules in this case is 4.
  - Assume that Access IDs 4, 5, 6 are bound to ports: 11-20, this is another unique set of rules and the count of additional rules will be 3.
  - In addition, Access IDs 5, 6 are bound to ports: 21-30, this is another unique set of rules and the count of additional rules will be 2.
  - Totally in the system there are: **4 + 3 + 2 = 9 rules!**

NOTE: ACL with action of Rate Limit can be applied only on one portt/LAG at a time.

This type of ACL is treated by the system as a unique ACL on each port it is bound to, so all the rules on a portt/LAG which has an ACL with Rate Limit action will be counted and consumed hardware resources.

From this reason, ACLs with Rate Limit action should be used very carefully, since the system maximum rule capacity can be reached if the user (for example) applies this rule on 240 ports. (which is less then the capacity of a full 6 unit stack of 48 ports switches.)

A

CONNECTORS AND CABLES

This section describes the devices physical interfaces and provides information about cable connections. Stations are connected to the device ports through the physical interface ports on the front panel, whereas devices are connected to create stacking by connecting the HDMI interface ports located on back panel.
. The following pin connectors are described:

- Pin Connections for the 10/100/1000 Ethernet Interface
- Pin Connections for the HDMI Connector

Pin Connections for the 10/100/1000 Ethernet Interface

The switching port can connect to stations wired with standard RJ-45 Ether straight or crossed cables.
The following figure illustrates the pin allocation.

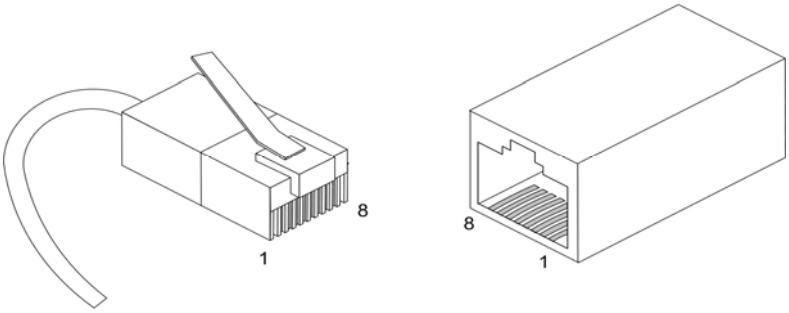


Figure A-1 RJ-45 Pin Allocation

RJ-45 Ports Pinout

The following table describes the pin allocation of the RJ-45 and the console ports:

PIN	SIGNAL NAME
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx 3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

Table 2: RJ-45 Pin Assignments

Pin Connections for the HDMI Connector

The stacking ports are used for connecting units using a standard HDMI cable.
The following figure illustrates the HDMI connector pin allocation:

Figure A-2 HDMI Pin Allocation

HDMI Ports Pinout

The following table describes the pin allocation of the HDMI connector:

PIN	SIGNAL NAME	PIN	SIGNAL NAME
1	TMDS Data 2+	11	TMDS Clock Shield
2	TMDS Data 2 Shield	12	TMDS Clock-
3	TMDS Data 2	13	CEC
4	TMDS Data 1+	14	No Connect
5	TMDS Data 1 Shield	15	DDC Clock
6	TMDS Data 1-	16	DDC Data
7	TMDS Data 0+	17	Ground
8	TMDS Data 0 Shield	18	+5V Power
9	TMDS Data 0-	19	Hot Plug Detect
10	TMDS Clock+	20	SHELL

Table 3: HDMI Pin Assignments

B

SYSLOG ERRORS

The Syslog Error Message Table displays a list of Syslog error messages appearing on the Switch according to level of severity and category, while providing a description for each error. There are seven levels of severity which are based on a hierarchy of severities. “Emergency” is the highest and “Debug” is the lowest. The user can only configure “All”, “Informational” and “Warning”. When a user configures a specific level, it applies to the configured level and all the levels above. For example, if a user defines an “Information” error message, it will apply to all messages from the “Informational” severity level up to the “Critical” level.

The seven severity levels are:

- 1. Critical
- 2. Warning
- 3. Error
- 4. Alert
- 5. Notice
- 6. Informational
- 7. Debug
- All – Represents Debug and above.

The following table displays the Syslog Error Messages:

Table 4: Syslog Error Message Table

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
SYSLG6.4.0	Critical		%(1)s	
SYSLG8.16.10	Critical		No memory 1	
SYSLG8.16.11	Critical		No memory 2	
SYSLG8.16.16	Critical	web	No free connection at the moment - wait one minute and retry.	Currently there is no free connection available. Wait one minute and retry.
SYSLG8.16.17	Critical	System	No free memory	No free memory available.
SYSLG8.16.18	Critical	System	No free UDP port	The system must be restarted.
SYSLG8.16.29	Critical	System	Cannot create private memory pool	Cannot create a private memory pool.
SYSLG8.16.31	Critical	AAA	Session amount exceeded	Session amount exceeded.
SYSLG8.16.6	Critical	Up/Download	Illegal file type	Illegal file type.
SYSLG8.16.9	Critical	Up/Download	Duplication of file name	A file name is duplicated.
SYSLG8.47.35	Critical	IP	Select master IP failed on ifIndex %(1)j@	Selected master IP failed on the specified ifIndex.
SYSLG8.47.37	Critical	IP	Primary IP address could not be obtained@	Primary IP address could not be obtained.
SYSLG8.47.8	Critical		Table is empty@	The table is empty.
SYSLG8.49.22	Critical		sshTlp_packet_read_packet: Padding error - need %(1)d block %(2)d mod %(3)d	
SYSLG8.49.24	Critical	SSH	sshTlp_kex_setup:	Insufficient memory

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			Insufficient memory to perform key exchange.	available to perform a key exchange.
SYSLG8.63.10	Critical	Stack	UNIT ID %(1)d,Msg:%(2)s	
SYSLG8.63.2	Critical	Stack	UNIT ID %(1)d,Trap:%(2)s	
SYSLG8.74.46	Critical	System	Cannot allocate memory for %(1)s	
SYSLG8.74.48	Critical	System	Create area %(1)s - cannot be inserted to list	The created specified area cannot be inserted into the list.
SYSLG8.16.16	Critical	web	No free connection at the moment - wait one minute and retry.	Currently there is no free connection available. Wait one minute and retry.
SYSLG8.16.17	Critical	System	No free memory	No free memory available.
SYSLG8.16.18	Critical	System	No free UDP port	The system must be restarted.
SYSLG8.16.29	Critical	System	Cannot create private memory pool	Cannot create a private memory pool.
SYSLG8.16.31	Critical	AAA	Session amount exceeded	Session amount exceeded.
SYSLG8.16.6	Critical	Up/Download	Illegal file type	Illegal file type.
SYSLG8.16.9	Critical	Up/Download	Duplication of file name	A file name is duplicated.
SYSLG8.47.35	Critical	IP	Select master IP failed on ifIndex %(1)j@	Selected master IP failed on the specified ifIndex.
SYSLG8.47.37	Critical	IP	Primary IP address could not be obtained@	Primary IP address could not be obtained.
SYSLG8.47.8	Critical		Table is empty@	The table is empty.
SYSLG8.49.22	Critical		sshTlp_packet_read_packet: Padding error - need %(1)d block %(2)d mod %(3)d	
SYSLG8.49.24	Critical	SSH	sshTlp_kex_setup: Insufficient memory to perform key exchange.	Insufficient memory available to perform a key exchange.
SYSLG8.63.10	Critical	Stack	UNIT ID %(1)d,Msg:%(2)s	
SYSLG8.63.2	Critical	Stack	UNIT ID %(1)d,Trap:%(2)s	
SYSLG8.74.46	Critical	System	Cannot allocate memory for %(1)s	
SYSLG8.74.48	Critical	System	Create area %(1)s - cannot be inserted to list	The created specified area cannot be inserted into the list.
SYSLG1.0.50	Error	IP	Invalid TFTP server IP Address, or Invalid / missing Instruction filename : %(1)s. Auto Update aborted.	Invalid TFTP server IP Address, or Invalid / missing instruction in the specified file name. The Auto Update process is

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
				aborted.
SYSLG1.0.51	Error	Up/Download	Failed to download the instruction File %(1)s. Auto Update aborted.	Failed to download the specified instruction File. The Auto Update process is aborted.
SYSLG1.0.52	Error	Up/Download	Failed to download File %(1)s. Auto Update aborted.	Failed to download specified file. The Auto Update process is aborted.
SYSLG1.0.53	Error	Up/Download	Failed to download File %(1)s. Auto Update aborted.@ reason : %(2)s	Failed to download specified file. The Auto Update process is aborted because of the specified reason.
SYSLG1.0.54	Error	AAA	Copy failed. Please verify that the configuration line in the instruction matches the name of the configuration file and that file exists on the server.	Copy failed. Please verify that the configuration line in the instruction matches the name of the configuration file and that file exists on the server.
SYSLG1.0.60	Error	Up/Download	Invalid auto update instruction file. Auto update aborted	The auto update instruction file is invalid. The Auto update process is aborted.
SYSLG1.0.61	Error	AAA	Can't restore factory defaults during auto update operation	The system could not restore the factory defaults during the auto update operation.
SYSLG1.5.21	Error	Stack	Lost connection with unit %(1)d reason 0x%(2)x. Unit will be rebooted .	Connection with the specified unit has been lost due to the specified reason. The unit will be rebooted.
SYSLG1.5.22	Error	Stack	Unit %(1)d was shutdown.	The specified unit was shutdown.
SYSLG4.10.1	Error		Transmission failed	Transmission has failed.
SYSLG4.11.0	Error	System	Reset to asic num %(1)d failed	The specified ASIC reset has failed.
SYSLG4.14.16	Error	System	Failed to get TAPI software version	Failed to get the TAPI software version.
SYSLG4.14.17	Error	System	Failed to get CORE software version	Failed to get the CORE software version.
SYSLG4.15.5	Error		%(1)s: Wrong mdix operative status	The mdix operative status is wrong.
SYSLG4.15.7	Error	Interface	ifIndex %(1)d - operation mode %(2)s	
SYSLG5.1.0	Error		%(1)s: Status %(2)s, value %(3)d	
SYSLG5.1.29	Error	VLAN	Failed to add entry for vlan %(1)d, mac %(2)s	Failed to add an entry for the specified VLAN and specified MAC address.
SYSLG5.1.30	Error	VLAN	Failed to delete entry for vlan %(1)d, mac %(2)s	Failed to delete an entry for the specified VLAN and

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
				specified MAC address.
SYSLG5.4.0	Error	Interface	SW3P_callback_rx_frame : Unknown frame encapsulation	Unknown frame encapsulation.
SYSLG6.0.0	Error	Up/Download	Boot image download aborted	The Boot image download process is aborted.
SYSLG6.0.10	Error	Up/Download	Flash programming failed	Flash programming has failed.
SYSLG6.0.11	Error	Security	Block programming failed	The Block programming process failed.
SYSLG6.0.4	Error	Up/Download	Boot image code file is too long	Boot image code file is too long.
SYSLG6.0.6	Error		Illegal format	Illegal format encountered.
SYSLG6.0.7	Error	Up/Download	The received file is not valid - download again!	The file received is invalid. The file needs to be downloaded again.
SYSLG6.0.8	Error	Up/Download	Boot1 programming failed, it is not valid any more	The Boot1 programming process failed, because it is not valid any more.
SYSLG6.0.9	Error	Up/Download	Boot2 programming failed, it is not valid any more	The Boot2 programming process failed, because it is not valid any more.
SYSLG7.0.121	Error	System	Memory overflow	There has been a memory overflow.
SYSLG7.0.130	Error	FDB	No free mac address	There is no free MAC address.
SYSLG7.0.78	Error	SNMP	Port %(1)j doesn't accept administrative parameter %(2)s@	The specified administrative parameter is not accepted.
SYSLG7.0.79	Error	Interface	Port %(1)j doesn't support %(2)s parameter@	The specified parameter is not supported.
SYSLG7.0.97	Error	VLAN	Memory overflow while creating the aggregateVlan Table@	Memory overflowed while creating the aggregate VLAN table.
SYSLG8.100.30	Error		Unable to synchronize a backup - dmanager problem: error - %(1)s, function - %(2)s	The Master is unable to synchronize the backup with the file. The data may be lost.
SYSLG8.100.32	Error	Up/Download	Wrong file version is received by backup unit.	Wrong file version is received by backup unit.
SYSLG8.100.33	Error	Up/Download	Wrong file size of backup unit.	The backup is not synchronized with a file.
SYSLG8.100.35	Error	Stack	The file update message from old master was received on backup unit. The file is ignored	The file update message from old master was received on backup unit. The file is ignored
SYSLG8.107.0	Error	FDB	Bad IGMP version@	The IGMP version is invalid.

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
SYSLG8.107.1	Error	VLAN	Bad vlan tag@	The VLAN tag is invalid.
SYSLG8.107.2	Error		Inconsistent vlan count@	Inconsistent VLAN count.
SYSLG8.108.1	Error	IP	IPL4GENG_init: UDP port reservation failed	The UDP port reservation has failed.
SYSLG8.110.12	Error	SNMP	received %(1)s interval is less than min value	The specified received interval is less than minimum value.
SYSLG8.110.13	Error	SNMP	calculated %(1)s interval is less than min value	The calculated specified interval is less than the minimum value.
SYSLG8.2.2	Error	System	Buffer allocation failed.	Buffer allocation failed.
SYSLG8.20.11	Error	IP	ARP Table Overflow	The ARP Table is full.
SYSLG8.20.13	Error	System	Init config failed	The initialization process failed.
SYSLG8.22.1	Error	IP	IP forwarding result is undefined	The IP forwarding result is undefined.
SYSLG8.26.1	Error	System	Errors occurred during initialization	Errors occurred during the initialization process.
SYSLG8.26.9	Error		%(1)s: Errors occurred during initialization	The specified errors occurred during the initialization process.
SYSLG8.31.12	Error	AAA	Authentication failed for %(1)s, source - %(2)s	
SYSLG8.31.29	Error	AAA	Radius returned attribute error	The RADIUS has found an erroneous attribute
SYSLG8.31.30	Error	SNMP	Unknown variable	Unknown code or status is encountered.
SYSLG8.31.31	Error	AAA	User name received empty string	The user name is an empty string
SYSLG8.45.15	Error	Up/Download	Creating/updating entry in copy history table failed	Failed to creating/update an entry in the Copy History table.
SYSLG8.45.21	Error	Up/Download	Could not add message to copy messages table	Could not add a message to the Copy Messages table.
SYSLG8.45.5	Error	System	COPYG_init: Errors occurred during init	Errors occurred during initialization.
SYSLG8.47.33	Error	IP	Primary IP Address %(1)s was deleted@	The specified primary IP address was deleted.
SYSLG8.49.1	Error	SSH	SSH error: %(1)s	
SYSLG8.49.16	Error	SSH	sshHostKeySave: DER formatted private key string too long (%(1)d bytes).@The key could not be saved to flash.	The DER formatted private key string too long. The key could not be saved to flash.
SYSLG8.49.21	Error	SSH	sshAuthpTreatMessage: Unable to allocate connection	Unable to allocate a connection.

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
SYSLG8.49.3	Error	SSH	Unable to allocate memory pool for SSH	Unable to allocate a memory pool for SSH.
SYSLG8.49.30	Error	SSH	sshp_text_handler: Unable to allocate memory for incoming text from the ssh connection. Data may have been lost.	Unable to allocate memory for incoming text from the SSH connection. Data may have been lost.
SYSLG8.49.4	Error	System	balloc: could not allocate %(1)d bytes (%(2)d)	Could not allocate the specified bytes.
SYSLG8.49.5	Error	Port Security	bfree: Cannot free memory: block is corrupt	Cannot free memory: The memory block is corrupt.
SYSLG8.49.6	Error	Port Security	bfree: Freeing more memory than was used	More memory was used,
SYSLG8.5.143	Error	SNMP	Unknown field %(1)s	The specified field is unknown.
SYSLG8.5.158	Error	System	Cannot update Hash	Cannot update the Hash.
SYSLG8.5.160	Error	System	Cannot clean Hash	Cannot clean the Hash values.
SYSLG8.5.161	Error	System	Cannot insert entry to Hash	Cannot insert an entry into Hash.
SYSLG8.5.162	Error	System	Cannot delete entry from Hash	Cannot delete an entry from Hash.
SYSLG8.5.180	Error	System	GCLIP_mib2cli_analyze_ command: Cannot insert entry to Hash	Cannot insert an entry to Hash.
SYSLG8.5.181	Error	SNMP	Length is limited by 160 characters	The field length is limited by 160 characters.
SYSLG8.56.3	Error	Interface	Failed to set default priority@	Failed to set default priority.
SYSLG8.58.4	Error	Security	Failed to update queue@	Failed to update queue.
SYSLG8.6.6	Error	VLAN	Too Many Vlan.	Too many VLANs are defined.
SYSLG8.61.0	Error		%(1)s: Errors occurred during initialization	Errors occurred during initialization.
SYSLG8.63.11	Error	Stack	UNIT ID %(1)d,Msg:%(2)s	
SYSLG8.63.3	Error	Stack	UNIT ID %(1)d,Trap:%(2)s	
SYSLG8.73.1	Error	System	Errors occurred during initialization	Errors occurred during the initialization process.
SYSLG8.74.57	Error	SSH	Packet RX on interface %(1)s from %(2)s type %(3)s - %(4)s	Key IDs do not match; keys are expired or some other key configuration problems.
SYSLG8.74.58	Error	SSH	Packet RX on virtual interface %(1)s area %(2)s type %(3)s - %(4)s	Key IDs do not match; keys are expired or some other key configuration problems.
SYSLG8.75.1	Error	IP	SVNZIP encountered data	SVNZIP encountered the

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			error %(1)d in the file %(2)s	specified data error in the specified file.
SYSLG8.75.11	Error	Web	PGPRCS: Failed to open the page %(1)s - in <PGPRCSP_createPageBuffer>.	Failed to open the specified page.
SYSLG8.75.12	Error	Web	You must give the "html/" path as parameter@	The "html/" path must be given as a parameter.
SYSLG8.75.13	Error		We support up to %(1)d different paths.@	Up to the specified number of paths are supported.
SYSLG8.75.14	Error	Up/Download	Could not open the txt file you supplied@	The supplied text file could not be opened.
SYSLG8.75.15	Error	Web	EmbWeb init: error initializing The WebServer@	Error occurred initializing the WebServer.
SYSLG8.75.16	Error	Web	WEBSRVG_task: Failure fetching from pipe@	Failure fetching data from a pipe.
SYSLG8.75.17	Error	Web	WEBUTILG_snprintf: result too big	The WEBUTILG_snprintf result is too large.
SYSLG8.75.2	Error	IP	SVNZIP out of memory extracting file %(1)s	SVNZIP process encountered memory problems while extracting the specified file.
SYSLG8.75.21	Error		%(1)s	
SYSLG8.75.3	Error	IP	SVNZIP found CRC Error extracting file %(1)s	SVNZIP found a CRC error while extracting the specified file.
SYSLG8.75.33	Error	Web	PGPRCS: Found no end tag, between two tags.	No end tag, encountered between two tags.
SYSLG8.75.4	Error	IP	Can't get hostname	A hostname cannot be received.
SYSLG8.75.43	Error	Web	PGPRCS: Trying to set tag %(1)s which does not exist in the page	Trying to set the specified tag which does not exist in the page.
SYSLG8.75.5	Error	Web	GOAHEADG: Received illegal buffer length in HTTP Post request	Received an illegal buffer length error in an HTTP Post request.
SYSLG8.75.59	Error		WARNING - The "if-modified-since" date can not be taken from the system so it will be set to 1/1/1970	WARNING - The "if-modified-since" date can not be taken from the system so it will be set to 1/1/1970
SYSLG8.75.6	Error		Bad %(1)s pointer	The specified pointer is invalid.
SYSLG8.75.60	Error	Web	The HTTP Buffer sent is to big.@ The buffer size can be up to %(1)d bytes@	The HTTP Buffer sent is to big The buffer size can be up to the specified number of bytes.
SYSLG8.75.61	Error		WB_KERN: in WEBSRVG_sendSslGoA	

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			head got post header chunk without Content Length Attribute.@	
SYSLG8.75.62	Error	IP	SVNZIP found an error %(1)u extracting file %(2)s	SVNZIP found an error while extracting the specified file.
SYSLG8.75.63	Error	IP	SVNZIP file %(1)s not found	The specified SVNZIP file not found.
SYSLG8.75.65	Error	IP	EmbWeb init: error initializing The UPNP BIN File@	Error occurred initializing the UPNP BIN file.
SYSLG8.75.67	Error	Web	PGPRCS: Field posted value exceeded allowed size.@	Posted field value exceeded the allowed size.
SYSLG8.75.68	Error	Web	GOAHEADG: Received illegal length (%(1)d) for field (%(2)s) in HTTP request.@	In the HTTP request the specified field length is illegal.
SYSLG8.75.69	Error	Web	GOAHEADG: Received illegal URL in HTTP request.@	Received an illegal URL in an HTTP request.
SYSLG8.75.7	Error	IP	GOAHEADG: Couldn't open a socket on port %(1)d - Will open the socket on port %(2)d@	Could not open a socket on the specified port. The socket will be opened on the second specified port.
SYSLG8.75.70	Error	Web	GOAHEADG: Received HTTP header request exceeded allowed size.@	Received an HTTP header request to exceeded allowed size.
SYSLG8.75.71	Error	Web	GOAHEADG: Couldn't find web service struct entry.@	Could not find a web service struct entry.
SYSLG8.75.72	Error	Web	GOAHEADG: Couldn't create web service struct entry.@	Could not create a web service struct entry.
SYSLG8.75.74	Error	Web	GOAHEADG: missing HTTP file transfer mandatory Data.@	Missing mandatory HTTP file transfer data.
SYSLG8.75.75	Error	Web	GOAHEADG: Failed to Reserve Port %(1)d on System Initialization.@	Failed to reserve the specified port while the system is initialized.
SYSLG8.75.8	Error	IP	GOAHEADG: Couldn't open a socket on ports %(1)d - %(2)d	Could not open a socket on the specified ports.
SYSLG8.75.80	Error	Web	Listener port %(1)u configured for WEB service %(2)s is not available@	The specified Listener port configured for the specified WEB service is not available.
SYSLG8.77.25	Error	System	Cannot add new session - DB overflow!	Cannot add new session because of the DB overflow.

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
SYSLG8.78.8	Error	System	Cannot allocate memory for user	The system cannot allocate memory for user.
SYSLG8.78.9	Error	System	Cannot create timer for user	The system cannot create a timer for user.
SYSLG8.83.5	Error	Up/Download	Backup %(1)d failed during runtime configuration @	The specified backup failed during runtime configuration.
SYSLG8.85.0	Error	Security	Unknown source received	An unknown source is received.
SYSLG8.85.1	Error	Web	Translation from url to name had failed	Translation from URL to name had failed.
SYSLG8.86.1	Error	SNMP	The enterprise given for trap is too long.	The given enterprise for trap is too long.
SYSLG8.86.2	Error	SSH	Not enough space for key of variable %(1)lu of trap %(2)lu.	There is not enough space for the key of the specified variable of the specified trap.
SYSLG8.86.26	Error		Memory not freed - SNMP Package: %(1)s Routine: %(2)d Location: %(3)d Size: %(4)d Unfreed block: %(5)s	
SYSLG8.86.29	Error		SNMP Package: %(1)s Routine: %(2)d Location: %(3)d Error: %(4)s	
SYSLG8.86.3	Error	SNMP	Not enough space for instance id of variable %(1)lu of trap %(2)lu.	There is not enough space for the instance ID of the specified variable of the specified trap.
SYSLG8.86.7	Error		SNMPCOMMG_StoreInitialCommunityEntry : no free community entry available	No free community entry is available.
SYSLG8.89.6	Error	SNMP	Unexpected entry fields were found in CDB, variable %(1)s	Unexpected entry fields were found in the specified CDB, and specified variable.
SYSLG8.89.7	Error	System	MIB variable %(1)lu not supported	The specified MIB variable is not supported.
SYSLG8.90.0	Error	AAA	Keymanager: Failed to send to backup	Failed to send to backup.
SYSLG8.90.1	Error	SSH	Keymanager: Size of the data exceeded	Size of the data exceeded.
SYSLG8.94.15	Error	System	Init: %(1)s	
SYSLG8.96.10	Error	Interface	Autogeneration of self-signed certificate was failed	Autogeneration of self-signed certificate has failed.
SYSLG8.97.17	Error	System	Buffer for notifying applicaton %(1)s could not be allocated.	The buffer for notifying the specified application could not be allocated.

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
SYSLG8.97.18	Error	System	Memory for notifying applicaton %(1)s could not be allocated.	Memory for notifying the specified application could not be allocated.
SYSLG1.0.55	Informational	Up/Download	File %(1)s has been Auto Updated	The specified file has been Auto Updated.
SYSLG1.0.56	Informational	Up/Download	Auto Update Completed; rebooting the switch	Auto Update is completed. The switch is being; rebooted.
SYSLG1.0.59	Informational	Up/Download	Active image successfully changed to image %(1)d	Active image is successfully changed to the specified image.
SYSLG1.2.4	Informational		entity configuration change trap.	
SYSLG1.3.0	Informational	Interface	Pse Port %(1)s delivering power to the PD.@	The specified PSE port is delivering power to the PD.
SYSLG1.3.1	Informational	System	PSE power usage %(1)d in unit %(2)d is above the threshold.@	The PSE power used by the specified unit is above the threshold.
SYSLG1.3.2	Informational	System	PSE power usage %(1)d in unit %(2)d is below the threshold.@	The PSE power used by the specified unit is below the threshold.
SYSLG1.5.23	Informational	Interface	Unit %(1)d was shutdown - JUMBO frames not supported.	The specified unit is shutdown because Jumbo frames are not supported.
SYSLG1.5.24	Informational	Stack	Master switchover: unit %(1)d is now master.	The specified unit is now the Master unit.
SYSLG1.5.25	Informational	Stack	Backup master unit %(1)d was removed from the stack.	The specified backup master is removed from the stack.
SYSLG1.5.26	Informational	Stack	Unit %(1)d was removed from the stack.	The specified unit is removed from the stack.
SYSLG1.5.28	Informational	IP	Ipc connection with unit %(1)d failed.	The IPC connection with the specified unit has failed.
SYSLG1.5.29	Informational		Configuration changed: %(1)s	
SYSLG1.5.30	Informational	Stack	Stack cable %(1)s : link %(2)s on unit-%(3)d	The specified stacking cable is connected to the specified unit.
SYSLG1.6.11	Informational		PS# %(1)d status changed - %(2)s.	The system uses two power supply sources: #1 and #2. The system can operate with one or both power supply units. The power supply has changed.
SYSLG1.6.8	Informational	System	FAN# %(1)d status changed - %(2)s.	The specified fan status has changed.
SYSLG4.10.13	Informational		Add dynamic MAC %(1)m - Vlan %(2)d failed, %(3)d mac failed to be inserted from the last	

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			trap	
SYSLG4.15.16	Informational		%(1)s %(2)s port %(3)s	
SYSLG4.15.18	Informational	Interface	Media changed from %(1)s to %(2)s on port %(3)s.	There has been a media change on the specified port.
SYSLG4.18.2	Informational	Security	Shaper cannot be applied on port %(1)s since it's working in half duplex. It will be applied when the port changes to full duplex.@	Shaper cannot be applied on the specified port because it is working in half duplex. It will be applied when the port changes to full duplex.
SYSLG4.6.9	Informational		%(1)s of port %(3)j differ from %(1)s of %(4)j	
SYSLG5.3.11	Informational		Activating service %(1)d	
SYSLG6.0.2	Informational	Up/Download	Boot image download started	The system supports the boot image update. A new file can be downloaded from a TFTP server. The message appears when this procedure starts.
SYSLG6.0.3	Informational	Up/Download	Boot image download completed	The Boot image download is completed successfully. The system supports the boot image update. A new file can be downloaded from a TFTP server. The message appears when this procedure is completed successfully.
SYSLG6.1.1	Informational		Port %(1)lu Up	
SYSLG6.2.1	Informational	Power	Power Supply #%(1)d is up	The system uses two power supply sources: #1 and #2. The system can operate with one or both power supply units. The specified power supply is up.
SYSLG7.0.0	Informational		%(1)s %(2)s	
SYSLG7.0.1	Informational		%(1)s %(2)s	
SYSLG7.13.0	Informational	1x	Port %(1)j is Authorized	The specified port is authorized.
SYSLG7.13.26	Informational	1x	MAC %(1)m is authorized on port %(2)j	The specified MAC is authorized on the specified port.
SYSLG7.15.0	Informational	Security	Port %(1)s suspended by Loopback Detection.@	The specified port is suspended by Loopback Detection.

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
SYSLG7.2.0	Informational	Interface	Port %(1)j added to %(2)j	A physical port is added to a logical link that is called a trunk, LAG, or channel depending on the device.
SYSLG7.2.46	Informational	1x	Port %(1)j can not be added to %(2)j: Unauthorized	
SYSLG7.5.64	Informational	IP	Dynamic port %(2)j was added to VLAN %(1)j by GVRP	A dynamically configured port was added to a VLAN during a GVRP protocol operation.
SYSLG7.5.65	Informational	VLAN	Dynamic port %(2)j was removed from VLAN %(1)j by GVRP	A dynamically configured port was removed from a VLAN during a GVRP protocol operation.
SYSLG7.5.66	Informational	VLAN	Dynamic VLAN %(1)j was added by GVRP	A dynamically configured VLAN was added during a GVRP protocol operation.
SYSLG7.5.67	Informational	VLAN	Dynamic VLAN %(1)j was removed by GVRP	A dynamically configured VLAN was removed during a GVRP protocol operation.
SYSLG7.5.68	Informational		VLAN %(1)j changed from Dynamic to Static	A dynamically configured VLAN was deleted from the list of dynamic VLANs and was then added to the statically configured VLANs during a GVRP protocol operation.
SYSLG7.5.69	Informational		VLAN %(1)j changed from Static to Dynamic	A statically configured VLAN was deleted from the list of static VLANs and was then added to the dynamically configured VLANs during a GVRP protocol operation.
SYSLG7.8.11	Informational		%(1)s	
SYSLG7.8.12	Informational		%(1)s	
SYSLG7.8.13	Informational	SSH	Failed to allocated memory for key	The system did not provide sufficient memory for the key.
SYSLG8.10.37	Informational	bootup	The device has been configured via BOOTP	The device has been configured via BOOTP.
SYSLG8.10.38	Informational	DHCP	The device has been configured on interface %(1)j , IP %(2)y, mask %(3)y, DHCP server %(4)y	The device has been configured on the specified interface, with the specified IP address and mask on the specified DHCP server.
SYSLG8.101.6	Informational	IP	ARP packet dropped from port %(1)j with VLAN tag %(2)d and reason:	ARP Inspection Log. The ARP packet is dropped according to the specified

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			%(3)s@SRC MAC %(4)m SRC IP %(5)y DST MAC %(6)m DST IP %(7)y	reason
SYSLG8.15.0	Informational		Ping completion status: %(1)s	
SYSLG8.15.1	Informational		Ping completion status:%(1)s.Sent:%(2)u.Received:%(3)u.Times:Min %(4)u,Max %(5)u,Avg %(6)u	
SYSLG8.17.0	Informational		%(1)s-%(2)s-%(3)s %(4)s:%(5)s:%(6)s %%TELNETD-I-CONNECTION, telnet connection from %(7)s at %(8)s-%(9)s-%(10)s %(11)s:%(12)s:%(13)s	
SYSLG8.26.2	Informational		Warm Startup	Warm Startup: the system re-initialization with no changes in configuration.
SYSLG8.26.3	Informational	Up/Download	Cold Startup	Cold Startup: the system re-initialization with possible changes in configuration.
SYSLG8.26.4	Informational	Up/Download	All NVRAM sections are erased	The system supports a few NVRAM sections. Each user can access its NVRAM section only. All data from all user sections can be deleted from NVRAM; then NVRAM is set to default values.
SYSLG8.26.5	Informational		NVRAM section %(1)s is erased	The system supports a few NVRAM users. Each user can access its NVRAM section only. A given user section can be erased from NVRAM.
SYSLG8.26.7	Informational	System	Initialization task is completed	The system informs that tasks are created and ready to be run by GO functions.
SYSLG8.31.0	Informational	AAA	New request to create user	The application must authenticate a new user.
SYSLG8.31.1	Informational	AAA	User created successfully	A new user is created in the current table of authenticated users.
SYSLG8.31.11	Informational	AAA	Authentication succeeded	Authentication with the current method succeeded.
SYSLG8.31.3	Informational	AAA	Request for authentication	The user authentication process is started.
SYSLG8.31.40	Informational	AAA	New %(1)s connection for user %(2)s, source %(5)s%(3)y destination	A new connection for the specified user between the specified source and

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			%(5)s%(4)y ACCEPTED	destination addresses is accepted.
SYSLG8.31.43	Informational	AAA	%(1)s connection for user %(2)s, source %(5)s%(3)y destination %(5)s%(4)y TERMINATED	A connection for the specified user between the specified source and destination addresses is terminated.
SYSLG8.31.46	Informational	AAA	AAA FILE overflow. Compression is perfomred. Within a compression not valid records are deleted.	The AAA file is full. Compression is performed during which invalid records are deleted.
SYSLG8.31.5	Informational	AAA	Method being retried	Authentication with the current method failed, and authentication is repeated once more by using the same method.
SYSLG8.31.6	Informational		Method succeeded	Authentication with the current method succeeded – an access is granted.
SYSLG8.31.63	Informational	AAA	User CLI session for user %(2)s over %(1)s , source %(3)y destination %(5)s %(4)y TERMINATED. The Telnet/SSH session may still be connected.	The CLI session for the specified user between the specified source and destination addresses is terminated. The Telnet/SSH session may still be connected.
SYSLG8.31.64	Informational	AAA	User CLI session for user %(2)s over %(1)s , source %(3)y destination %(5)s %(4)y ACCEPTED	The CLI session for the specified user between the specified source and destination addresses is accepted.
SYSLG8.31.7	Informational	AAA	Method failed	
SYSLG8.31.8	Informational	AAA	Method error	
SYSLG8.45.18	Informational	Up/Download	Files Copy - source URL %(1)s destination URL %(2)s	The files are copied from the specified source address to the specified destination address.
SYSLG8.48.31	Informational	STP	Attention: port %(1)j from which the bpdu was received is configured as Fast Port	A received BPDU message indicates that the specified port is configured as the Fast port..
SYSLG8.49.11	Informational		sshpClientId: illegal connection id %(1)d	
SYSLG8.49.14	Informational	Security	Closed SSH connection to %(1)y	
SYSLG8.49.2	Informational	SSH	SSH log: %(1)s	The string parameter describes the reason this message was called.

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
SYSLG8.49.9	Informational	AAA	sshpClientFind: illegal index %(1)d	
SYSLG8.5.168	Informational	console	MIB variable %(1)s not found in temporary DB	The specified MIB variable was not found in the Mib2cli temporary DB.
SYSLG8.5.169	Informational	SNMP	Unknown field name %(1)s	The SNMPServG_name_2_Id function failed because MIB variable name is unknown.
SYSLG8.5.170	Informational	console	Command Handler for command ID %(1)s is missing	The command handler for the specified command ID is missing.
SYSLG8.5.171	Informational	console	Command <%(1)s> processed in %(2)d.%(3)d secs	It took the specified number of seconds to process the specified command.
SYSLG8.50.18	Informational	Interface	Port changed status from notPresent to notPresent@	An indication of not present port when this port is already not present is wrong.
SYSLG8.63.14	Informational	Stack	UNIT ID %(1)d,Msg:%(2)s	(Valid for stackable projects only) See the relevant trap message as in the case when the specified stack member operating in the standalone mode issues it.
SYSLG8.63.6	Informational	Stack	UNIT ID %(1)d,Trap:%(2)s	(Valid for stackable projects only) See the relevant trap message as in the case when the specified stack member operating in the standalone mode issues it.
SYSLG8.74.51	Informational	Interface	Interface %(1)s state %(2)s	
SYSLG8.74.52	Informational	Interface	Virtual interface %(1)s area %(2)s state %(3)s	
SYSLG8.79.5	Informational	Web	File Delete - file URL %(1)s	The file at the specified URL has been deleted.
SYSLG8.83.2	Informational	Stack	Synchronization with unit %(1)d is failed @	Synchronization with the specified unit has failed.
SYSLG8.83.3	Informational	Stack	Synchronization with unit %(1)d is finished successfully @	Synchronization with the specified unit has succeeded.
SYSLG8.83.4	Informational	Stack	Wrong source unit id %(1)d, message discarted @	The specified source unit ID is incorrect, the message is discarded.
SYSLG8.84.0	Informational	IP	NTP Packet received from UDP	The NTP packet is received from the UDP.
SYSLG8.84.5	Informational		Illegal data size	The data size is too large.

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
SYSLG8.84.9	Informational		NTP received - Mode %(1)d, src_ip %(2)s, dst_ip %(3)s, Interface %(4)d@	
SYSLG8.86.30	Informational	SNMP	SNMP Package: %(1)s Routine: %(2)d Location: %(3)d Error: %(4)s	
SYSLG8.86.31	Informational		Syslog testing logging of UINT_64 parameters: %(1)u %(2)i %(3)d %(4)x %(5)X	
SYSLG8.86.8	Informational	Up/Download	Number of %(2)s configuration items loaded: %(1)lu	The specified number of configuration commands has been loaded.
SYSLG8.92.1	Informational	Up/Download	XMODEM session has been aborted@	The XModem session is aborted.
SYSLG8.92.2	Informational	Up/Download	XMODEM session has been completed@	The XModem session is ended.
SYSLG8.95.10	Informational	Up/Download	Configuration Download has been started	The configuration file download process has started.
SYSLG8.95.3	Informational	Up/Download	Configuration Upload has been completed	The configuration file upload process has been successfully completed.
SYSLG8.95.4	Informational	Up/Download	Configuration Download has been completed	The configuration file download process has been successfully completed.
SYSLG8.95.9	Informational	Up/Download	Configuration Upload has been started	The configuration file upload process has started.
SYSLG8.96.8	Informational		Starting autogeneration of self-signed certificate - %(1)u bits	
SYSLG8.96.9	Informational	AAA	Autogeneration of self-signed certificate was successfully completed	The Autogeneration for a self-signed certificate was successfully completed
SYSLG1.0.55	Informational	Up/Download	File %(1)s has been Auto Updated	The specified file has been Auto Updated.
SYSLG1.0.56	Informational	Up/Download	Auto Update Completed; rebooting the switch	Auto Update is completed. The switch is being; rebooted.
SYSLG1.0.59	Informational	Up/Download	Active image successfully changed to image %(1)d	Active image is successfully changed to the specified image.
SYSLG1.2.4	Informational		entity configuration change trap.	
SYSLG1.3.0	Informational	Interface	Pse Port %(1)s delivering power to the PD.@	The specified PSE port is delivering power to the PD.
SYSLG1.3.1	Informational	System	PSE power usage %(1)d in unit %(2)d is above the	The PSE power used by the specified unit is above the

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			threshold.@	threshold.
SYSLG1.3.2	Informational	System	PSE power usage %(1)d in unit %(2)d is below the threshold.@	The PSE power used by the specified unit is below the threshold.
SYSLG1.5.23	Informational	Interface	Unit %(1)d was shutdown - JUMBO frames not supported.	The specified unit is shutdown because Jumbo frames are not supported.
SYSLG1.5.24	Informational	Stack	Master switchover: unit %(1)d is now master.	The specified unit is now the Master unit.
SYSLG1.5.25	Informational	Stack	Backup master unit %(1)d was removed from the stack.	The specified backup master is removed from the stack.
SYSLG1.5.26	Informational	Stack	Unit %(1)d was removed from the stack.	The specified unit is removed from the stack.
SYSLG1.5.28	Informational	IP	Ipc connection with unit %(1)d failed.	The IPC connection with the specified unit has failed.
SYSLG1.5.29	Informational		Configuration changed: %(1)s	
SYSLG1.5.30	Informational	Stack	Stack cable %(1)s : link %(2)s on unit-%(3)d	The specified stacking cable is connected to the specified unit.
SYSLG1.6.11	Informational		PS# %(1)d status changed - %(2)s.	The system uses two power supply sources: #1 and #2. The system can operate with one or both power supply units. The power supply has changed.
SYSLG1.6.8	Informational	System	FAN# %(1)d status changed - %(2)s.	The specified fan status has changed.
SYSLG4.10.13	Informational		Add dynamic MAC %(1)m - Vlan %(2)d failed, %(3)d mac failed to be inserted from the last trap	
SYSLG4.15.16	Informational		%(1)s %(2)s port %(3)s	
SYSLG4.15.18	Informational	Interface	Media changed from %(1)s to %(2)s on port %(3)s.	There has been a media change on the specified port.
SYSLG4.18.2	Informational	Security	Shaper cannot be applied on port %(1)s since it's working in half duplex. It will be applied when the port changes to full duplex.@	Shaper cannot be applied on the specified port because it is working in half duplex. It will be applied when the port changes to full duplex.
SYSLG4.6.9	Informational		%(1)s of port %(3)j differ from %(1)s of %(4)j	
SYSLG5.3.11	Informational		Activating service %(1)d...	
SYSLG6.0.2	Information	Up/Download	Boot image download	The system supports the

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
	al		started	boot image update. A new file can be downloaded from a TFTP server. The message appears when this procedure starts.
SYSLG6.0.3	Informational	Up/Download	Boot image download completed	The Boot image download is completed successfully. The system supports the boot image update. A new file can be downloaded from a TFTP server. The message appears when this procedure is completed successfully.
SYSLG6.1.1	Informational		Port %(1)lu Up	
SYSLG6.2.1	Informational	Power	Power Supply #%(1)d is up	The system uses two power supply sources: #1 and #2. The system can operate with one or both power supply units. The specified power supply is up.
SYSLG7.0.0	Informational		%(1)s %(2)s	
SYSLG7.0.1	Informational		%(1)s %(2)s	
SYSLG7.13.0	Informational	1x	Port %(1)j is Authorized	The specified port is authorized.
SYSLG7.13.26	Informational	1x	MAC %(1)m is authorized on port %(2)j	The specified MAC is authorized on the specified port.
SYSLG7.15.0	Informational	Security	Port %(1)s suspended by Loopback Detection.@	The specified port is suspended by Loopback Detection.
SYSLG7.2.0	Informational	Interface	Port %(1)j added to %(2)j	A physical port is added to a logical link that is called a trunk, LAG, or channel depending on the device.
SYSLG7.2.46	Informational	1x	Port %(1)j can not be added to %(2)j: Unauthorized	
SYSLG7.5.64	Informational	IP	Dynamic port %(2)j was added to VLAN %(1)j by GVRP	A dynamically configured port was added to a VLAN during a GVRP protocol operation.
SYSLG7.5.65	Informational	VLAN	Dynamic port %(2)j was removed from VLAN %(1)j by GVRP	A dynamically configured port was removed from a VLAN during a GVRP protocol operation.
SYSLG7.5.66	Informational	VLAN	Dynamic VLAN %(1)j was added by GVRP	A dynamically configured VLAN was added during a GVRP protocol operation.

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
SYSLG7.5.67	Informational	VLAN	Dynamic VLAN %(1)j was removed by GVRP	A dynamically configured VLAN was removed during a GVRP protocol operation.
SYSLG7.5.68	Informational		VLAN %(1)j changed from Dynamic to Static	A dynamically configured VLAN was deleted from the list of dynamic VLANs and was then added to the statically configured VLANs during a GVRP protocol operation.
SYSLG7.5.69	Informational		VLAN %(1)j changed from Static to Dynamic	A statically configured VLAN was deleted from the list of static VLANs and was then added to the dynamically configured VLANs during a GVRP protocol operation.
SYSLG7.8.11	Informational		%(1)s	
SYSLG7.8.12	Informational		%(1)s	
SYSLG7.8.13	Informational	SSH	Failed to allocated memory for key	The system did not provide sufficient memory for the key.
SYSLG8.10.37	Informational	bootup	The device has been configured via BOOTP	The device has been configured via BOOTP.
SYSLG8.10.38	Informational	DHCP	The device has been configured on interface %(1)j , IP %(2)y, mask %(3)y, DHCP server %(4)y	The device has been configured on the specified interface, with the specified IP address and mask on the specified DHCP server.
SYSLG8.101.6	Informational	IP	ARP packet dropped from port %(1)j with VLAN tag %(2)d and reason: %(3)s@SRC MAC %(4)m SRC IP %(5)y DST MAC %(6)m DST IP %(7)y	ARP Inspection Log. The ARP packet is dropped according to the specified reason
SYSLG8.15.0	Informational		Ping completion status: %(1)s	
SYSLG8.15.1	Informational		Ping completion status:%(1)s.Sent:%(2)u.Received:%(3)u.Times:Min %(4)u,Max %(5)u,Avg %(6)u	
SYSLG8.17.0	Informational		%(1)s-%(2)s-%(3)s %(4)s:%(5)s:%(6)s %%TELNETD-I-CONNECTION, telnet connection from %(7)s at %(8)s-%(9)s-%(10)s %(11)s:%(12)s:%(13)s	
SYSLG8.26.2	Information		Warm Startup	Warm Startup: the system

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
	al			re-initialization with no changes in configuration.
SYSLG8.26.3	Informational	Up/Download	Cold Startup	Cold Startup: the system re-initialization with possible changes in configuration.
SYSLG8.26.4	Informational	Up/Download	All NVRAM sections are erased	The system supports a few NVRAM sections. Each user can access its NVRAM section only. All data from all user sections can be deleted from NVRAM; then NVRAM is set to default values.
SYSLG8.26.5	Informational		NVRAM section %(1)s is erased	The system supports a few NVRAM users. Each user can access its NVRAM section only. A given user section can be erased from NVRAM.
SYSLG8.26.7	Informational	System	Initialization task is completed	The system informs that tasks are created and ready to be run by GO functions.
SYSLG8.31.0	Informational	AAA	New request to create user	The application must authenticate a new user.
SYSLG8.31.1	Informational	AAA	User created successfully	A new user is created in the current table of authenticated users.
SYSLG8.31.11	Informational	AAA	Authentication succeeded	Authentication with the current method succeeded.
SYSLG8.31.3	Informational	AAA	Request for authentication	The user authentication process is started.
SYSLG8.31.40	Informational	AAA	New %(1)s connection for user %(2)s, source %(5)s%(3)y destination %(5)s%(4)y ACCEPTED	A new connection for the specified user between the specified source and destination addresses is accepted.
SYSLG8.31.43	Informational	AAA	%(1)s connection for user %(2)s, source %(5)s%(3)y destination %(5)s%(4)y TERMINATED	A connection for the specified user between the specified source and destination addresses is terminated.
SYSLG8.31.46	Informational	AAA	AAA FILE overflow. Compression is perfomred. Within a compression not valid records are deleted.	The AAA file is full. Compression is performed during which invalid records are deleted.
SYSLG8.31.5	Informational	AAA	Method being retried	Authentication with the current method failed, and authentication is repeated once more by using the same method.
SYSLG8.31.6	Information		Method succeeded	Authentication with the

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
	al			current method succeeded – an access is granted.
SYSLG8.31.63	Informational	AAA	User CLI session for user %(2)s over %(1)s , source %(3)y destination %(5)s %(4)y TERMINATED. The Telnet/SSH session may still be connected.	The CLI session for the specified user between the specified source and destination addresses is terminated. The Telnet/SSH session may still be connected.
SYSLG8.31.64	Informational	AAA	User CLI session for user %(2)s over %(1)s , source %(3)y destination %(5)s %(4)y ACCEPTED	The CLI session for the specified user between the specified source and destination addresses is accepted.
SYSLG8.31.7	Informational	AAA	Method failed	
SYSLG8.31.8	Informational	AAA	Method error	
SYSLG8.45.18	Informational	Up/Download	Files Copy - source URL %(1)s destination URL %(2)s	The files are copied from the specified source address to the specified destination address.
SYSLG8.48.31	Informational	STP	Attention: port %(1)j from which the bpdu was received is configured as Fast Port	A received BPDU message indicates that the specified port is configured as the Fast port..
SYSLG8.49.11	Informational		sshpClientId: illegal connection id %(1)d	
SYSLG8.49.14	Informational	Security	Closed SSH connection to %(1)y	
SYSLG8.49.2	Informational	SSH	SSH log: %(1)s	The string parameter describes the reason this message was called.
SYSLG8.49.9	Informational	AAA	sshpClientFind: illegal index %(1)d	
SYSLG8.5.168	Informational	console	MIB variable %(1)s not found in temporary DB	The specified MIB variable was not found in the Mib2cli temporary DB.
SYSLG8.5.169	Informational	SNMP	Unknown field name %(1)s	The SNMPServG_name_2_Id function failed because MIB variable name is unknown.
SYSLG8.5.170	Informational	console	Command Handler for command ID %(1)s is missing	The command handler for the specified command ID is missing.
SYSLG8.5.171	Informational	console	Command <%(1)s> processed in %(2)d.%(3)d secs	It took the specified number of seconds to process the specified command.
SYSLG8.50.18	Informational	Interface	Port changed status from notPresent to notPresent@	An indication of not present port when this port is

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
				already not present is wrong.
SYSLG8.63.14	Informational	Stack	UNIT ID %(1)d,Msg:%(2)s	(Valid for stackable projects only) See the relevant trap message as in the case when the specified stack member operating in the standalone mode issues it.
SYSLG8.63.6	Informational	Stack	UNIT ID %(1)d,Trap:%(2)s	(Valid for stackable projects only) See the relevant trap message as in the case when the specified stack member operating in the standalone mode issues it.
SYSLG8.74.51	Informational	Interface	Interface %(1)s state %(2)s	
SYSLG8.74.52	Informational	Interface	Virtual interface %(1)s area %(2)s state %(3)s	
SYSLG8.79.5	Informational	Web	File Delete - file URL %(1)s	The file at the specified URL has been deleted.
SYSLG8.83.2	Informational	stack	Synchronization with unit %(1)d is failed @	Synchronization with the specified unit has failed.
SYSLG8.83.3	Informational	Stack	Synchronization with unit %(1)d is finished successfully @	Synchronization with the specified unit has succeeded.
SYSLG8.83.4	Informational	Stack	Wrong source unit id %(1)d, message discarted @	The specified source unit ID is incorrect, the message is discarded.
SYSLG8.84.0	Informational	IP	NTP Packet received from UDP	The NTP packet is received from the UDP.
SYSLG8.84.5	Informational		Illegal data size	The data size is too large.
SYSLG8.84.9	Informational		NTP received - Mode %(1)d, src_ip %(2)s, dst_ip %(3)s, Interface %(4)d@	
SYSLG8.86.30	Informational	SNMP	SNMP Package: %(1)s Routine: %(2)d Location: %(3)d Error: %(4)s	
SYSLG8.86.31	Informational		Syslog testing logging of UINT_64 parameters: %(1)u %(2)i %(3)d %(4)x %(5)X	
SYSLG8.86.8	Informational	Up/Download	Number of %(2)s configuration items loaded: %(1)lu	The specified number of configuration commands has been loaded.
SYSLG8.92.1	Informational	Up/Download	XMODEM session has been aborted@	The XModem session is aborted.
SYSLG8.92.2	Informational	Up/Download	XMODEM session has been completed@	The XModem session is ended.

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
SYSLG7.14.0	Notice		LLDP status: %(1)s.	
SYSLG8.1.0	Notice		Bad msg received from %(1)y on intf %(2)y	
SYSLG8.1.1	Notice		Ignoring msg from %(1)y on intf %(2)y	
SYSLG8.105.1	Notice	IP	IP FDB Table Overflow : %(1)s@	The IP FDB Table is full..
SYSLG8.16.2	Notice	Web	Session is closed after timeout is expired	Session is closed after timeout period is reached.
SYSLG8.26.6	Notice		NVRAM section %(1)s not found and cannot be erased	The specified NVRAM section not found and cannot be erased.
SYSLG8.45.7	Notice	Up/Download	The copy operation was completed successfully	The copy operation completed successfully.
SYSLG8.63.13	Notice	Stack	UNIT ID %(1)d,Msg:%(2)s	
SYSLG8.63.5	Notice	Stack	UNIT ID %(1)d,Trap:%(2)s	
SYSLG8.89.1	Notice	SNMP	Start conversion of old format CDB	The conversion of old format CDB has started.
SYSLG8.89.2	Notice	SNMP	End conversion of old format CDB	The conversion of old format CDB has finished.
SYSLG8.9.10	Notice	Interface	Type %(1)u not supported	The specified type is not supported.
SYSLG8.9.12	Notice		Illegal chksum, igmp_size = %(1)lu	
SYSLG7.14.0	Notice		LLDP status: %(1)s.	
SYSLG8.1.0	Notice		Bad msg received from %(1)y on intf %(2)y	
SYSLG8.1.1	Notice		Ignoring msg from %(1)y on intf %(2)y	
SYSLG8.105.1	Notice	IP	IP FDB Table Overflow : %(1)s@	The IP FDB Table is full..
SYSLG8.16.2	Notice	Web	Session is closed after timeout is expired	Session is closed after timeout period is reached.
SYSLG8.26.6	Notice		NVRAM section %(1)s not found and cannot be erased	The specified NVRAM section not found and cannot be erased.
SYSLG8.45.7	Notice	Up/Download	The copy operation was completed successfully	The copy operation completed successfully.
SYSLG8.63.13	Notice	Stack	UNIT ID %(1)d,Msg:%(2)s	
SYSLG8.63.5	Notice	Stack	UNIT ID %(1)d,Trap:%(2)s	
SYSLG8.89.1	Notice	SNMP	Start conversion of old format CDB	The conversion of old format CDB has started.
SYSLG8.89.2	Notice	SNMP	End conversion of old	The conversion of old

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			format CDB	format CDB has finished.
SYSLG8.9.10	Notice	Interface	Type %(1)u not supported	The specified type is not supported.
SYSLG8.9.12	Notice		Illegal chksum, igmp_size = %(1)lu	
SYSLG1.0.32	Warning	Interface	You may need to set interface %(1)s to force full duplex and appropriate speed to match partner link configuration.	The specified interface may need to be set to force full duplex and appropriate speed to match partner link configuration.
SYSLG1.6.10	Warning	Power	PS# %(1)d status changed - %(2)s.	The specified port status has changed.
SYSLG4.5.3	Warning	Port Security	A packet with source MAC %(1)m tried to access through port %(2)j which is locked@	A security violation warning is issued to a user who activated a port as locked. When data from a new MAC address arrives to such port, a trap is sent.
SYSLG4.5.34	Warning	1x	A packet with source MAC %(1)m tried to access through port %(2)j which is authorize and multiple-host disable@	A packet with a specified MAC address attempted to gain access through a port which requires authorization and which is disabled for multiple hosts.
SYSLG5.3.10	Warning	Interface	Sum of the committed BW on interface %(1)d is more than port speed, all the services applied to it will scaled down.	The sum of the committed BW on the specified interface d is more than port speed, all the services applied to it will scaled down.
SYSLG5.3.12	Warning	Security	Service %(1)d is partially active, up to interface %(2)d.	The specified Service is partially active, up to a specified interface.
SYSLG5.3.13	Warning	Security	Service %(1)d can't be active because of erroneous %(2)s.	The specified Service cannot be active because of the specified errors.
SYSLG5.3.14	Warning		BW (in kbits) %(1)d, has %(2)s to trunk %(3)d	
SYSLG5.3.17	Warning	Security	Activating non-guarantee service %(1)d with ignored egress interfaces.	Activating non-guarantee specified services with ignored egress interfaces.
SYSLG5.3.18	Warning	Security	Drop profile in host parameter %(1)d is bigger than the asic maximum number %(2)d	Drop profile in specified host parameter is bigger than the ASIC maximum specified number.
SYSLG5.3.5	Warning	Interface	IfIndex %(1)d is now auto negotiation enable.	The specified IfIndex is now auto negotiation enabled.
SYSLG5.3.6	Warning	Interface	IfIndex %(1)d is configured with auto	The specified IfIndex is configured with auto

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			negotiation enable.	negotiation enabled.
SYSLG5.3.7	Warning	Interface	Committing BW on egress interface %(1)d more than %(2)d percentages of interface speed.	Committing BW on the specified egress interface d more than the specified percentages of interface speed.
SYSLG5.3.8	Warning	Interface	Interface %(1)d changes to half duplex mode, some committed services can't be fulfilled.	The specified interface changes to half duplex mode and some committed services cannot be fulfilled.
SYSLG5.3.9	Warning	Interface	Interface %(1)d changes to higher speed rate. Current speed (in Kbit)%(2)d.	The specified interface speed is modified to a higher speed.
SYSLG6.1.0	Warning		Port %(1)lu Down	
SYSLG6.2.0	Warning	Power	Power Supply #%(1)d is down	The specified power supply is down. The system uses two power supply sources: #1 and #2. The system can operate with one or both power supply units.
SYSLG7.0.161	Warning		%(1)s %(2)s	
SYSLG7.0.2	Warning		%(1)s %(2)s	
SYSLG7.0.3	Warning		%(1)s %(2)s	
SYSLG7.0.4	Warning		%(1)s %(2)s	
SYSLG7.0.5	Warning		%(1)s %(2)s	
SYSLG7.0.6	Warning		%(1)s %(2)s	
SYSLG7.0.7	Warning		%(1)s %(2)s	
SYSLG7.0.8	Warning		%(1)s %(2)s	
SYSLG7.0.9	Warning		%(1)s %(2)s	
SYSLG7.10.8	Warning	Security	failed to allocate rules in Asic for ifIndex %(1)d @	Failed to allocate ASIC rules in a specified change.
SYSLG7.10.9	Warning	Security	failed to add %(1)d rules to the Asic on ifIndex %(2)d @	Failed to add the specified rules to the ASIC on the specified ifIndex .
SYSLG7.13.1	Warning	1x	Port %(1)j is unAuthorized	The specified port is un authorized.
SYSLG7.13.27	Warning	FDB	MAC %(1)m was rejected on port %(2)j	The specified MAC address was rejected on the specified port.
SYSLG7.14.107	Warning	SNMP	LLDP %(1)s Warning: - Deleting Mngmnt address entry from CDB was failed: resource unavailable.@	The management address entry deletion from CDB failed. Resource are unavailable.
SYSLG7.2.1	Warning	Interface	Port %(1)j removed from %(2)j	The specified port is removed.
SYSLG7.2.2	Warning	Interface	Port %(1)j removed from	The specified port is

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			%(2)j: port is down/notPresent	removed and is indicated as being down or not present.
SYSLG8.0.4	Warning	IP	Network IP address %(1)s is unavailable	The IP address was most likely allocated statically.
SYSLG8.1.31	Warning	STP	Active change failed - unreachable route not added because of Routing table overflow	The message appears when topology changes took place but the system failed to add an entry to the table because no memory is available.
SYSLG8.10.14	Warning	bootup	BOOTP client received illegal IP mask in BOOTP msg	The BOOTP client received an illegal IP mask in the BOOTP message.
SYSLG8.10.15	Warning	DHCP	DHCP client received illegal IP mask in DHCP msg	The DHCP client received an illegal IP mask in DHCP message.
SYSLG8.10.16	Warning	bootup	BOOTP client received illegal IP address in BOOTP msg	The BOOTP client received an illegal IP address in the BOOTP message.
SYSLG8.10.17	Warning	DHCP	DHCP client received illegal IP address in DHCP msg	The DHCP client received an illegal IP address in the DHCP message.
SYSLG8.10.20	Warning	bootup	BOOTP msg indicates that IP interface and default router are not on the same subnet	Error in the BOOTP server configuration where the IP interface and default router are not on the same subnet.
SYSLG8.10.21	Warning	bootup	BOOTP msg indicates that IP interface and TFTP server are not on the same subnet	Error in the BOOTP server configuration where the IP interface and TFTP server are not on the same subnet.
SYSLG8.10.22	Warning	DHCP	DHCP msg on interface %(1)j indicates that IP interface %(2)y and default router %(2)y, mask %(3)y, are not on the same subnet	Error in the DHCP server configuration where the specified IP interface and specified default router with the specified mask are not on the same subnet.
SYSLG8.10.23	Warning	DHCP	DHCP msg on interface %(1)j indicates that default router %(2)y, mask %(3)y, sent by DHCP server %(4)y is either a subnet name or a broadcast	Error in the DHCP server configuration where the specified IP interface and specified default router with the specified mask are broadcast.
SYSLG8.10.24	Warning	DHCP	DHCP msg indicates that IP interface and TFTP server are not on the same subnet	Error in the DHCP server configuration where the IP interface and TFTP server are not on the same subnet.
SYSLG8.10.25	Warning	bootup	BOOTP msg indicates that file name was configured without configuring IP address of TFTP server	A BOOTP message must include a TFTP server IP address.
SYSLG8.10.26	Warning	IP	IP address of TFTP server	The TFTP server IP address

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			is not configured	must be configured.
SYSLG8.10.27	Warning	IP	BOOTP client received file with too long name in BOOTP msg	A file name is composed of a limited number of characters as defined in the system.
SYSLG8.10.28	Warning	DHCP	DHCP client received file with too long name in DHCP msg	A file name is composed of a limited number of characters as defined in the system.
SYSLG8.10.29	Warning	AAA	Illegal auth protocol type %(1)u	Illegal authentication protocol type has been received in the DHCP Message Log.
SYSLG8.10.30	Warning	AAA	Illegal privacy required value %(1)u	Illegal required privacy is received in the DHCP Message Log.
SYSLG8.10.31	Warning	bootup	Authentication key change via BOOTP/DHCP client not allowed	The Authentication key change via BOOTP/DHCP client is not allowed.
SYSLG8.10.32	Warning	bootup	Privacy key change via BOOTP/DHCP client not allowed	A Privacy key change via BOOTP/DHCP client not allowed.
SYSLG8.10.33	Warning	SSH	Privacy key change required	A Privacy key change is required.
SYSLG8.10.34	Warning	AAA	Privacy Key change length (%(1)u) does not fit privacy protocol	The modified Privacy Key length does not fit the privacy protocol.
SYSLG8.10.35	Warning	AAA	Authentication password required	An authentication key is received, but not configured.
SYSLG8.10.36	Warning	SSH	Privacy password required	A Privacy password change is required.
SYSLG8.10.39	Warning	DHCP	The device has rejected an invalid IP configuration on interface %(1)j , IP %(2)y, mask %(3)y, DHCP server %(4)y	The device has rejected an invalid IP configuration on the specified interface with the specified mask and DHCP server.
SYSLG8.10.40	Warning	DHCP	The device has rejected a duplicated subnet configuration on interface %(1)j, IP %(2)y, mask %(3)y, DHCP server %(4)y	The device has rejected a duplicated subnet configuration on the specified interface with the specified mask and DHCP server.
SYSLG8.10.41	Warning	DHCP	Malformed DHCP packet √ Message type option was found in DHCP packet	A abnormal DHCP packet message type option was found in the DHCP packet.
SYSLG8.10.8	Warning	IP	BOOTP client received illegal magic cookie %(1)x%(2)x%(3)x%(4)x(%(5)x%(6)x%(7)x%(8)x - must be	The 4-byte value of the received cookie must match the 4-byte value of the legal cookie.

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			%(1)x%(2)x%(3)x%(4)x(%(5)x%(6)x%(7)x%(8)x	
SYSLG8.10.9	Warning	IP	DHCP client received illegal magic cookie %(1)x%(2)x%(3)x%(4)x(%(5)x%(6)x%(7)x%(8)x - must be %(1)x%(2)x%(3)x%(4)x(%(5)x%(6)x%(7)x%(8)x	The 4-byte value of the received cookie must match the 4-byte value of the legal cookie.
SYSLG8.100.11	Warning	IP	DHCP snooping received illegal magic cookie %(1)x%(2)x%(3)x%(4)x(%(5)x%(6)x%(7)x%(8)x - must be %(1)x%(2)x%(3)x%(4)x(%(5)x%(6)x%(7)x%(8)x	The 4-byte value of the received cookie must match the 4-byte value of the legal cookie.
SYSLG8.109.1	Warning		%(1)s@	
SYSLG8.16.25	Warning	FDB	Unexpected PDU code	Packet is corrupted and will be discarded.
SYSLG8.31.2	Warning	AAA	Cannot create a user	A user cannot be authenticated because of AAA low resources.
SYSLG8.31.36	Warning	AAA	Received unsupported authentication REPLY msg status=%(1)u (server msg: %(2)s)	Received a message indicating that authentication method is unsupported.
SYSLG8.31.37	Warning	AAA	Unsupported arguments for adding received in authorization RESPONSE msg: %(1)s	Received a message indicating the additional authentication argument is not supported.
SYSLG8.31.38	Warning	AAA	Unsupported arguments for replacement received in authorization RESPONSE msg: %(1)s	Received a message indicating the replacement authentication argument is not supported.
SYSLG8.31.39	Warning	AAA	Received unsupported authentication RESPONSE msg status = %(1)u	Received a message indicating authentication is not supported.
SYSLG8.31.41	Warning	AAA	New %(1)s connection for user %(2)s, source %(5)s%(3)y destination %(5)s%(4)y REJECTED	
SYSLG8.31.42	Warning	AAA	User %(1)s LOCKED after unsuccessful login from %(2)s, source %(5)s%(3)y destination %(5)s%(4)y	The specified user ID is locked after an unsuccessful login from the specified source to the specified destination.
SYSLG8.31.44	Warning	AAA	AAA FILE data corruption occurs. Valid data ONLY saved	AAA data corruption has occurred. All valid data has been saved.
SYSLG8.40.13	Warning	Security	%(1)s Packet dropped by Policy rule no.%(2)s .	The packet is dropped in accordance with the

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
				specified security criteria.
SYSLG8.40.14	Warning	Security	%(1)s Packet forward by Policy rule no.%(2)s .	The specified packet is forward by the specified Policy rule.
SYSLG8.43.10	Warning	IP	TFTP connection cannot be started without IP address	Configuration error. The TFTP connection cannot be started without an IP address.
SYSLG8.43.7	Warning	Up/Download	Empty file downloaded, configuration unchanged	Configuration file is empty.
SYSLG8.44.0	Warning	FDB	IGMP Filter table is overflowed	The IGMP Filter table is full.
SYSLG8.44.1	Warning	FDB	Failed to insert entry to IGMP Filter table	Entries cannot be added to the table that a user has access to because the platform reached its limit.
SYSLG8.45.8	Warning	Up/Download	The copy operation has failed	The copy operation has failed.
SYSLG8.45.9	Warning	Up/Download	The configuration file has failed to download	The configuration file has failed to download.
SYSLG8.46.10	Warning	Security	Management ACL drop packet received on interface %(1)s%(2)j from %(3)y to %(4)y protocol %(5)d service %(6)s	A Management ACL drop packet is received on the specified interface.
SYSLG8.48.35	Warning	STP	%(1)j: STP status Blocking	STP status is in Blocking mode.
SYSLG8.48.36	Warning	STP	%(1)j: STP status Forwarding	STP status is in Forwarding mode.
SYSLG8.48.37	Warning	STP	%(1)j of instance %(2)d: STP status Blocking	For the specified instance the STP status is in Blocking mode.
SYSLG8.48.38	Warning	STP	%(1)j of instance %(2)d: STP status Forwarding	For the specified instance the STP status is in Forwarding mode.
SYSLG8.48.41	Warning	STP	%(1)j: STP Loopback Detection.	
SYSLG8.48.42	Warning	STP	%(1)j: STP Loopback Detection resolved.	
SYSLG8.49.10	Warning	AAA	sshpConId: connection %(1)d outside client range	Excessive number of clients serviced by the system.
SYSLG8.49.12	Warning	AAA	sshpClientId: connection id %(1)d is in the range reserved for channels	Excessive number of channels in the system.
SYSLG8.49.13	Warning	AAA	sshpClientId: connection %(1)d is outside the range reserved for clients	Excessive number of clients serviced by the system.
SYSLG8.49.51	Warning	SSH	The SSH daemon can not use the configured TCP port (the port is already	The SSH daemon cannot use the configured TCP port (the port is already being

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			being used).	used).
SYSLG8.49.52	Warning	AAA	Insufficient memory to generate an %(1)s key. Please close all SSH or SSL sessions and try again.	Insufficient memory to generate an authentication key. Close all SSH or SSL sessions and try again.
SYSLG8.49.7	Warning	SSH	SSH has been enabled but an encryption key was not found.@For key generation use the 'crypto key generate' commands. The service will start automatically when a host key is generated.	SSH has been enabled but an encryption key was not found. For key generation use the 'crypto key generate' commands. The service starts automatically when a host key is generated.
SYSLG8.5.190	Warning		%(1)s: %(2)s - no such expression variable	
SYSLG8.50.22	Warning	FDB	Failed to create multicast group entry of VLAN %(1)d MAC %(2)s@	The system resource to support this number of multicast entries is limited.
SYSLG8.51.0	Warning	FDB	IGMP group table overflow@	The IGMP group table is full.
SYSLG8.51.1	Warning	FDB	IGMP router table overflow@	The IGMP router table is full.
SYSLG8.51.10	Warning	FDB	IGMP Snooping: in version 3 received version 1 query msg	Version 3 IGMP Snooping received a Version 1 query message.
SYSLG8.51.11	Warning	FDB	IGMP Snooping: in version 3 received version 2 query msg	Version 3 IGMP Snooping received a Version 2 query message.
SYSLG8.51.39	Warning	FDB	BIGMPP_indication warning: Unknown value of frame type received for igmp snooping (%(1)d igmp control frames dropped from the last warning)@	Unknown frame type value received for IGMP snooping. The specified IGMP control frames are dropped from the last warning.
SYSLG8.51.5	Warning	FDB	IGMP Snooping: in version 1 received leave v2 msg	Version 1 IGMP Snooping received a Version 2 leave message.
SYSLG8.51.6	Warning	FDB	IGMP Snooping: in version 1 received version 2 query msg	Version 1 IGMP Snooping received a Version 2 query message.
SYSLG8.51.7	Warning	FDB	IGMP Snooping: in version 1 received version 3 query msg	Version 1 IGMP Snooping received a Version 3 query message.
SYSLG8.51.8	Warning	FDB	IGMP Snooping: in version 2 received version 3 query msg	Version 2 IGMP Snooping received a Version 3 query message.
SYSLG8.51.9	Warning	FDB	IGMP Snooping: in version 2 received version 1 query msg	Version 2 IGMP Snooping received a Version 1 query message.

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
SYSLG8.52.10	Warning	Port Security	Port Lock action on Mac Table has ended@	Port Lock action on the MAC Table has ended.
SYSLG8.52.2	Warning	FDB	Bridge forwarding table overflow@	The bridge forwarding table is full.
SYSLG8.52.6	Warning	FDB	BRMNP_nttb_hash_set_entry: Hash Insert Failed for VLAN: %(1)j Mac: %(2)s Port: %(3)j, Error: %(4)s	The MAC database is full. No entry can be inserted - the CPU memory limitations.
SYSLG8.52.9	Warning	Port Security	Port Lock action on Mac Table has started@	Port Lock action on the MAC Table has started.
SYSLG8.57.1	Warning	FDB	Bridge forwarding table overflow@	The bridge forwarding table is full.
SYSLG8.63.12	Warning	Stack	UNIT ID %(1)d,Msg:%(2)s	
SYSLG8.63.4	Warning	Stack	UNIT ID %(1)d,Trap:%(2)s	
SYSLG8.68.42	Warning	IP	Host and domain name size exceeds %(1)d bytes	Host and domain name size exceeds the specified number of bytes.
SYSLG8.74.55	Warning	Interface	Packet RX on interface %(1)s from %(2)s type %(3)s - %(4)s	Packets corrupted and (or) network problems.
SYSLG8.74.56	Warning	SSH	Packet RX on virtual interface %(1)s area %(2)s type %(3)s - %(4)s	Key IDs do not match; keys are expired or some other key configuration problems.
SYSLG8.74.60	Warning	SSH	Packet RX on virtual interface %(1)s area %(2)s type %(3)s - %(4)s	Key IDs do not match; keys are expired or some other key configuration problems.
SYSLG8.74.65	Warning	AAA	Packet TX from interface %(1)s - md5 auth key not found	Md5 keys are not found or are invalid.
SYSLG8.74.67	Warning	AAA	Packet TX from interface %(1)s - last authentication key has expired	Md5 keys are not found or are invalid.
SYSLG8.74.68	Warning	AAA	Packet RX on interface %(1)s from %(2)s - last authentication key has expired	Key IDs do not match; keys are expired or some other key configuration problems.
SYSLG8.75.0	Warning	Web	HTTPS server has been enabled but a certificate was not found.@For certificate generation use the - @ 'crypto certificate [1-2] generate' command.@The service will start automatically when a certificate is generated.	HTTPS server has been enabled but a certificate was not found. For a certificate generation use the - 'crypto certificate [1-2] generate' command. The service will start automatically when a certificate is generated.
SYSLG8.75.66	Warning		%(2)s service has been enabled but an encryption	The specified service has been enabled but an

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			key (certificate %(1)d) was not found.@For key generation use the 'crypto key generate' commands. The service will start automatically when a host key is generated.	encryption key was not found. For key generation use the 'crypto key generate' commands. The service starts automatically when a host key is generated.
SYSLG8.77.26	Warning	AAA	Invalid attribute %(1)d ignored - %(2)s	The specified attribute is ignored.
SYSLG8.78.14	Warning	AAA	Msg of %(1)u length received from server %(3)s is bigger than maximum - %(2)u. Information is truncated.	The message length is bigger than the specified maximum. Extra characters will be truncated.
SYSLG8.78.15	Warning	AAA	Parsing of the %(1)s msg received from TACACS server %(2)s failed	Parsing of the specified message received from the specified TACACS server has failed.
SYSLG8.78.18	Warning	IP	Unexpected TCP msg was received from server %(1)s	Unexpected TCP message was received from the specified server.
SYSLG8.78.2	Warning	AAA	No TACACS+ server is configured, cannot start authentication	No TACACS+ server is configured, so authentication cannot be performed.
SYSLG8.78.23	Warning	AAA	Connection to server %(1)s is aborted. Single Connection mode may not be supported by this server.	A connection attempt to a specified server is terminated. Single connection mode is not supported by the current server.
SYSLG8.78.6	Warning	AAA	No TACACS+ server is configured, cannot start authorization	No TACACS+ server is configured, so authorization cannot be started.
SYSLG8.78.7	Warning	AAA	Cannot create new user, too many users	Cannot create new user due to too many users already configured.
SYSLG8.79.4	Warning	Up/Download	FLMNGG_update_file_state: The entry of file %(1)s was not updated to the flash	The entry to the specified file was not updated to the flash.
SYSLG8.80.2	Warning	SNMP	PIMGLG_snmp_bindmib variable: For variable id %(1)lu the snmp operation %(2)s not supported.	For the specified variable ID the SNMP operation is not supported.
SYSLG8.81.12	Warning		Func=%(1)s:Line=%(2)d: %(3)s	
SYSLG8.81.14	Warning		Func=%(1)s:Line=%(2)d: Unknown return value %(3)d	
SYSLG8.81.18	Warning		Func=%(2)s:Line=%(1)d:	

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			Can't allocate buffer	
SYSLG8.81.19	Warning		Func=%(2)s:Line=%(1)d: No outgoing interface	
SYSLG8.81.20	Warning		%(1)s state mashine:State:%(2)s,Event:%(3)s:GroupIp=%(4)s,SrcIp=%(5)s received	
SYSLG8.81.21	Warning		%(1)s state mashine:Incompatible State:%(2)s,Event:%(3)s for GroupIp=%(4)s,SrcIp=%(5)s received	
SYSLG8.81.6	Warning	System	Module %(1)s: Call function %(2)s without init	In the specified module the specified call function is without initialization.
SYSLG8.81.7	Warning		%(1)s: Bad state in state machine %(2)s	The specified state is not correct is the specified state machine.
SYSLG8.81.8	Warning		%(1)s: Hash table %(2)s is full	The specified hash table is full.
SYSLG8.86.0	Warning	Up/Download	Configuration update of unit %(1)lu failed. Reason: %(2)s.	The specified unit configuration update failed.
SYSLG8.86.4	Warning	SNMP	Access attempted by unauthorized NMS	Access attempted by an unauthorized NMS.
SYSLG8.86.9	Warning	Up/Download	Error encountered while downloading config: %(1)s	An error occurred while downloading the specified configuration.
SYSLG8.89.8	Warning	SNMP	Overflow in CDB	There is an overflow in CDB.
SYSLG8.89.9	Warning	SNMP	Overflow in startup CDB. offset = %(1)lu, file end = %(2)lu	
SYSLG8.9.11	Warning	FDB	Timer allocation failed	The v1 Host Timer cannot be activated, and a router will stay in the v1 state.
SYSLG8.9.14	Warning	FDB	Querier->NonQueirier transition on Interface: %(1)j	An interface stopped to be a Querier.
SYSLG8.9.7	Warning	FDB	IGMP Cache table is overflowed	No entry can be inserted - the platform reached its limit.
SYSLG8.9.8	Warning	FDB	Received IGMP wrong version (V1) query	Received a wrong IGMP version (v1) query.
SYSLG8.9.9	Warning	FDB	Received IGMP wrong version (V2) query	Received a wrong IGMP version (v2) query
SYSLG8.95.0	Warning	Up/Download	Configuration upload has been aborted	Configuration file upload has been aborted.
SYSLG8.95.1	Warning	Up/Download	Configuration download	Configuration file

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			has been aborted	download has been aborted.
SYSLG8.95.6	Warning		%(1)s	
SYSLG8.96.7	Warning		Unknown certificate subject field	
SYSLG8.98.6	Warning	System	Bad OS status	Bad OS status.
SYSLG8.98.7	Warning	FDB	Reached Maximum number of IGMP memberships	The IGMP database is full. No entry can be inserted.
SYSLG1.0.32	Warning	Interface	You may need to set interface %(1)s to force full duplex and appropriate speed to match partner link configuration.	The specified interface may need to be set to force full duplex and appropriate speed to match partner link configuration.
SYSLG1.6.10	Warning	Power	PS# %(1)d status changed - %(2)s.	The specified port status has changed.
SYSLG4.5.3	Warning	Port Security	A packet with source MAC %(1)m tried to access through port %(2)j which is locked@	A security violation warning is issued to a user who activated a port as locked. When data from a new MAC address arrives to such port, a trap is sent.
SYSLG4.5.34	Warning	1x	A packet with source MAC %(1)m tried to access through port %(2)j which is authorize and multiple-host disable@	A packet with a specified MAC address attempted to gain access through a port which requires authorization and which is disabled for multiple hosts.
SYSLG5.3.10	Warning	Interface	Sum of the committed BW on interface %(1)d is more than port speed, all the services applied to it will scaled down.	The sum of the committed BW on the specified interface d is more than port speed, all the services applied to it will scaled down.
SYSLG5.3.12	Warning	Security	Service %(1)d is partially active, up to interface %(2)d.	The specified Service is partially active, up to a specified interface.
SYSLG5.3.13	Warning	Security	Service %(1)d can't be active because of erroneous %(2)s.	The specified Service cannot be active because of the specified errors.
SYSLG5.3.14	Warning		BW (in kbits) %(1)d, has %(2)s to trunk %(3)d	
SYSLG5.3.17	Warning	Security	Activating non-guarantee service %(1)d with ignored egress interfaces.	Activating non-guarantee specified services with ignored egress interfaces.
SYSLG5.3.18	Warning	Security	Drop profile in host parameter %(1)d is bigger than the asic maximum number %(2)d	Drop profile in specified host parameter is bigger than the ASIC maximum specified number.
SYSLG5.3.5	Warning	Interface	IfIndex %(1)d is now auto negotiation enable.	The specified IfIndex is now auto negotiation

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
				enabled.
SYSLG5.3.6	Warning	Interface	IfIndex %(1)d is configured with auto negotiation enable.	The specified IfIndex is configured with auto negotiation enabled.
SYSLG5.3.7	Warning	Interface	Committing BW on egress interface %(1)d more than %(2)d percentages of interface speed.	Committing BW on the specified egress interface d more than the specified percentages of interface speed.
SYSLG5.3.8	Warning	Interface	Interface %(1)d changes to half duplex mode, some committed services can't be fulfilled.	The specified interface changes to half duplex mode and some committed services cannot be fulfilled.
SYSLG5.3.9	Warning	Interface	Interface %(1)d changes to higher speed rate. Current speed (in Kbit)%(2)d.	The specified interface speed is modified to a higher speed.
SYSLG6.1.0	Warning		Port %(1)lu Down	
SYSLG6.2.0	Warning	Power	Power Supply #%(1)d is down	The specified power supply is down. The system uses two power supply sources: #1 and #2. The system can operate with one or both power supply units.
SYSLG7.0.161	Warning		%(1)s %(2)s	
SYSLG7.0.2	Warning		%(1)s %(2)s	
SYSLG7.0.3	Warning		%(1)s %(2)s	
SYSLG7.0.4	Warning		%(1)s %(2)s	
SYSLG7.0.5	Warning		%(1)s %(2)s	
SYSLG7.0.6	Warning		%(1)s %(2)s	
SYSLG7.0.7	Warning		%(1)s %(2)s	
SYSLG7.0.8	Warning		%(1)s %(2)s	
SYSLG7.0.9	Warning		%(1)s %(2)s	
SYSLG7.10.8	Warning	Security	failed to allocate rules in Asic for ifIndex %(1)d @	Failed to allocate ASIC rules in a specified change.
SYSLG7.10.9	Warning	Security	failed to add %(1)d rules to the Asic on ifIndex %(2)d @	Failed to add the specified rules to the ASIC on the specified ifIndex .
SYSLG7.13.1	Warning	1x	Port %(1)j is unAuthorized	The specified port is un authorized.
SYSLG7.13.27	Warning	FDB	MAC %(1)m was rejected on port %(2)j	The specified MAC address was rejected on the specified port.
SYSLG7.14.107	Warning	SNMP	LLDP %(1)s Warning: - Deleting Mngmnt address entry from CDB was failed: resource unavailable.@	The management address entry deletion from CDB failed. Resource are unavailable.

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
SYSLG7.2.1	Warning	Interface	Port %(1)j removed from %(2)j	The specified port is removed.
SYSLG7.2.2	Warning	Interface	Port %(1)j removed from %(2)j: port is down/notPresent	The specified port is removed and is indicated as being down or not present.
SYSLG8.0.4	Warning	IP	Network IP address %(1)s is unavailable	The IP address was most likely allocated statically.
SYSLG8.1.31	Warning	STP	Active change failed - unreachable route not added because of Routing table overflow	The message appears when topology changes took place but the system failed to add an entry to the table because no memory is available.
SYSLG8.10.14	Warning	bootup	BOOTP client received illegal IP mask in BOOTP msg	The BOOTP client received an illegal IP mask in the BOOTP message.
SYSLG8.10.15	Warning	DHCP	DHCP client received illegal IP mask in DHCP msg	The DHCP client received an illegal IP mask in DHCP message.
SYSLG8.10.16	Warning	bootup	BOOTP client received illegal IP address in BOOTP msg	The BOOTP client received an illegal IP address in the BOOTP message.
SYSLG8.10.17	Warning	DHCP	DHCP client received illegal IP address in DHCP msg	The DHCP client received an illegal IP address in the DHCP message.
SYSLG8.10.20	Warning	bootup	BOOTP msg indicates that IP interface and default router are not on the same subnet	Error in the BOOTP server configuration where the IP interface and default router are not on the same subnet.
SYSLG8.10.21	Warning	bootup	BOOTP msg indicates that IP interface and TFTP server are not on the same subnet	Error in the BOOTP server configuration where the IP interface and TFTP server are not on the same subnet.
SYSLG8.10.22	Warning	DHCP	DHCP msg on interface %(1)j indicates that IP interface %(2)y and default router %(2)y, mask %(3)y, are not on the same subnet	Error in the DHCP server configuration where the specified IP interface and specified default router with the specified mask are not on the same subnet.
SYSLG8.10.23	Warning	DHCP	DHCP msg on interface %(1)j indicates that default router %(2)y, mask %(3)y, sent by DHCP server %(4)y is either a subnet name or a broadcast	Error in the DHCP server configuration where the specified IP interface and specified default router with the specified mask are broadcast.
SYSLG8.10.24	Warning	DHCP	DHCP msg indicates that IP interface and TFTP server are not on the same subnet	Error in the DHCP server configuration where the IP interface and TFTP server are not on the same subnet.
SYSLG8.10.25	Warning	bootup	BOOTP msg indicates that file name was configured	A BOOTP message must include a TFTP server IP

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			without configuring IP address of TFTP server	address.
SYSLG8.10.26	Warning	IP	IP address of TFTP server is not configured	The TFTP server IP address must be configured.
SYSLG8.10.27	Warning	IP	BOOTP client received file with too long name in BOOTP msg	A file name is composed of a limited number of characters as defined in the system.
SYSLG8.10.28	Warning	DHCP	DHCP client received file with too long name in DHCP msg	A file name is composed of a limited number of characters as defined in the system.
SYSLG8.10.29	Warning	AAA	Illegal auth protocol type %(1)u	Illegal authentication protocol type has been received in the DHCP Message Log.
SYSLG8.10.30	Warning	AAA	Illegal privacy required value %(1)u	Illegal required privacy is received in the DHCP Message Log.
SYSLG8.10.31	Warning	bootup	Authentication key change via BOOTP/DHCP client not allowed	The Authentication key change via BOOTP/DHCP client is not allowed.
SYSLG8.10.32	Warning	bootup	Privacy key change via BOOTP/DHCP client not allowed	A Privacy key change via BOOTP/DHCP client not allowed.
SYSLG8.10.33	Warning	SSH	Privacy key change required	A Privacy key change is required.
SYSLG8.10.34	Warning	AAA	Privacy Key change length (%(1)u) does not fit privacy protocol	The modified Privacy Key length does not fit the privacy protocol.
SYSLG8.10.35	Warning	AAA	Authentication password required	An authentication key is received, but not configured.
SYSLG8.10.36	Warning	SSH	Privacy password required	A Privacy password change is required.
SYSLG8.10.39	Warning	DHCP	The device has rejected an invalid IP configuration on interface %(1)j , IP %(2)y, mask %(3)y, DHCP server %(4)y	The device has rejected an invalid IP configuration on the specified interface with the specified mask and DHCP server.
SYSLG8.10.40	Warning	DHCP	The device has rejected a duplicated subnet configuration on interface %(1)j, IP %(2)y, mask %(3)y, DHCP server %(4)y	The device has rejected a duplicated subnet configuration on the specified interface with the specified mask and DHCP server.
SYSLG8.10.41	Warning	DHCP	Malformed DHCP packet √ Message type option was found in DHCP packet	A abnormal DHCP packet message type option was found in the DHCP packet.
SYSLG8.10.8	Warning	IP	BOOTP client received	The 4-byte value of the

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			illegal magic cookie %(1)x%(2)x%(3)x%(4)x(%(5)x%(6)x%(7)x%(8)x - must be %(1)x%(2)x%(3)x%(4)x(%(5)x%(6)x%(7)x%(8)x	received cookie must match the 4-byte value of the legal cookie.
SYSLG8.10.9	Warning	IP	DHCP client received illegal magic cookie %(1)x%(2)x%(3)x%(4)x(%(5)x%(6)x%(7)x%(8)x - must be %(1)x%(2)x%(3)x%(4)x(%(5)x%(6)x%(7)x%(8)x	The 4-byte value of the received cookie must match the 4-byte value of the legal cookie.
SYSLG8.100.11	Warning	IP	DHCP snooping received illegal magic cookie %(1)x%(2)x%(3)x%(4)x(%(5)x%(6)x%(7)x%(8)x - must be %(1)x%(2)x%(3)x%(4)x(%(5)x%(6)x%(7)x%(8)x	The 4-byte value of the received cookie must match the 4-byte value of the legal cookie.
SYSLG8.109.1	Warning		%(1)s@	
SYSLG8.16.25	Warning	FDB	Unexpected PDU code	Packet is corrupted and will be discarded.
SYSLG8.31.2	Warning	AAA	Cannot create a user	A user cannot be authenticated because of AAA low resources.
SYSLG8.31.36	Warning	AAA	Received unsupported authentication REPLY msg status=%(1)u (server msg: %(2)s)	Received a message indicating that authentication method is unsupported.
SYSLG8.31.37	Warning	AAA	Unsupported arguments for adding received in authorization RESPONSE msg: %(1)s	Received a message indicating the additional authentication argument is not supported.
SYSLG8.31.38	Warning	AAA	Unsupported arguments for replacement received in authorization RESPONSE msg: %(1)s	Received a message indicating the replacement authentication argument is not supported.
SYSLG8.31.39	Warning	AAA	Received unsupported authentication RESPONSE msg status = %(1)u	Received a message indicating authentication is not supported.
SYSLG8.31.41	Warning	AAA	New %(1)s connection for user %(2)s, source %(5)s%(3)y destination %(5)s%(4)y REJECTED	
SYSLG8.31.42	Warning	AAA	User %(1)s LOCKED after unsuccessful login from %(2)s, source %(5)s%(3)y destination %(5)s%(4)y	The specified user ID is locked after an unsuccessful login from the specified source to the specified destination.
SYSLG8.31.44	Warning	AAA	AAA FILE data	AAA data corruption has

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			corruption occurs. Valid data ONLY saved	occurred. All valid data has been saved.
SYSLG8.40.13	Warning	Security	%(1)s Packet dropped by Policy rule no.%(2)s .	The packet is dropped in accordance with the specified security criteria.
SYSLG8.40.14	Warning	Security	%(1)s Packet forward by Policy rule no.%(2)s .	The specified packet is forward by the specified Policy rule.
SYSLG8.43.10	Warning	IP	TFTP connection cannot be started without IP address	Configuration error. The TFTP connection cannot be started without an IP address.
SYSLG8.43.7	Warning	Up/Download	Empty file downloaded, configuration unchanged	Configuration file is empty.
SYSLG8.44.0	Warning	FDB	IGMP Filter table is overflowed	The IGMP Filter table is full.
SYSLG8.44.1	Warning	FDB	Failed to insert entry to IGMP Filter table	Entries cannot be added to the table that a user has access to because the platform reached its limit.
SYSLG8.45.8	Warning	Up/Download	The copy operation has failed	The copy operation has failed.
SYSLG8.45.9	Warning	Up/Download	The configuration file has failed to download	The configuration file has failed to download.
SYSLG8.46.10	Warning	Security	Management ACL drop packet received on interface %(1)s%(2)j from %(3)y to %(4)y protocol %(5)d service %(6)s	A Management ACL drop packet is received on the specified interface.
SYSLG8.48.35	Warning	STP	%(1)j: STP status Blocking	STP status is in Blocking mode.
SYSLG8.48.36	Warning	STP	%(1)j: STP status Forwarding	STP status is in Forwarding mode.
SYSLG8.48.37	Warning	STP	%(1)j of instance %(2)d: STP status Blocking	For the specified instance the STP status is in Blocking mode.
SYSLG8.48.38	Warning	STP	%(1)j of instance %(2)d: STP status Forwarding	For the specified instance the STP status is in Forwarding mode.
SYSLG8.48.41	Warning	STP	%(1)j: STP Loopback Detection.	
SYSLG8.48.42	Warning	STP	%(1)j: STP Loopback Detection resolved.	
SYSLG8.49.10	Warning	AAA	sshpConId: connection %(1)d outside client range	Excessive number of clients serviced by the system.
SYSLG8.49.12	Warning	AAA	sshpClientId: connection id %(1)d is in the range reserved for channels	Excessive number of channels in the system.
SYSLG8.49.13	Warning	AAA	sshpClientId: connection %(1)d is outside the range	Excessive number of clients serviced by the system.

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			reserved for clients	
SYSLG8.49.51	Warning	SSH	The SSH daemon can not use the configured TCP port (the port is already being used).	The SSH daemon cannot use the configured TCP port (the port is already being used).
SYSLG8.49.52	Warning	AAA	Insufficient memory to generate an %(1)s key. Please close all SSH or SSL sessions and try again.	Insufficient memory to generate an authentication key. Close all SSH or SSL sessions and try again.
SYSLG8.49.7	Warning	SSH	SSH has been enabled but an encryption key was not found.@For key generation use the 'crypto key generate' commands. The service will start automatically when a host key is generated.	SSH has been enabled but an encryption key was not found. For key generation use the 'crypto key generate' commands. The service starts automatically when a host key is generated.
SYSLG8.5.190	Warning		%(1)s: %(2)s - no such expression variable	
SYSLG8.50.22	Warning	FDB	Failed to create multicast group entry of VLAN %(1)d MAC %(2)s@	The system resource to support this number of multicast entries is limited.
SYSLG8.51.0	Warning	FDB	IGMP group table overflow@	The IGMP group table is full.
SYSLG8.51.1	Warning	FDB	IGMP router table overflow@	The IGMP router table is full.
SYSLG8.51.10	Warning	FDB	IGMP Snooping: in version 3 received version 1 query msg	Version 3 IGMP Snooping received a Version 1 query message.
SYSLG8.51.11	Warning	FDB	IGMP Snooping: in version 3 received version 2 query msg	Version 3 IGMP Snooping received a Version 2 query message.
SYSLG8.51.39	Warning	FDB	BIGMPP_indication warning: Unknown value of frame type received for igmp snooping (%(1)d igmp control frames dropped from the last warning)@	Unknown frame type value received for IGMP snooping. The specified IGMP control frames are dropped from the last warning.
SYSLG8.51.5	Warning	FDB	IGMP Snooping: in version 1 received leave v2 msg	Version 1 IGMP Snooping received a Version 2 leave message.
SYSLG8.51.6	Warning	FDB	IGMP Snooping: in version 1 received version 2 query msg	Version 1 IGMP Snooping received a Version 2 query message.
SYSLG8.51.7	Warning	FDB	IGMP Snooping: in version 1 received version 3 query msg	Version 1 IGMP Snooping received a Version 3 query message.
SYSLG8.51.8	Warning	FDB	IGMP Snooping: in version 2 received version	Version 2 IGMP Snooping received a Version 3 query

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			3 query msg	message.
SYSLG8.51.9	Warning	FDB	IGMP Snooping: in version 2 received version 1 query msg	Version 2 IGMP Snooping received a Version 1 query message.
SYSLG8.52.10	Warning	Port Security	Port Lock action on Mac Table has ended@	Port Lock action on the MAC Table has ended.
SYSLG8.52.2	Warning	FDB	Bridge forwarding table overflow@	The bridge forwarding table is full.
SYSLG8.52.6	Warning	FDB	BRMNP_nttb_hash_set_entry: Hash Insert Failed for VLAN: %(1)j Mac: %(2)s Port: %(3)j, Error: %(4)s	The MAC database is full. No entry can be inserted - the CPU memory limitations.
SYSLG8.52.9	Warning	Port Security	Port Lock action on Mac Table has started@	Port Lock action on the MAC Table has started.
SYSLG8.57.1	Warning	FDB	Bridge forwarding table overflow@	The bridge forwarding table is full.
SYSLG8.63.12	Warning	Stack	UNIT ID %(1)d,Msg:%(2)s	
SYSLG8.63.4	Warning	Stack	UNIT ID %(1)d,Trap:%(2)s	
SYSLG8.68.42	Warning	IP	Host and domain name size exceeds %(1)d bytes	Host and domain name size exceeds the specified number of bytes.
SYSLG8.74.55	Warning	Interface	Packet RX on interface %(1)s from %(2)s type %(3)s - %(4)s	Packets corrupted and (or) network problems.
SYSLG8.74.56	Warning	SSH	Packet RX on virtual interface %(1)s area %(2)s type %(3)s - %(4)s	Key IDs do not match; keys are expired or some other key configuration problems.
SYSLG8.74.60	Warning	SSH	Packet RX on virtual interface %(1)s area %(2)s type %(3)s - %(4)s	Key IDs do not match; keys are expired or some other key configuration problems.
SYSLG8.74.65	Warning	AAA	Packet TX from interface %(1)s - md5 auth key not found	Md5 keys are not found or are invalid.
SYSLG8.74.67	Warning	AAA	Packet TX from interface %(1)s - last authentication key has expired	Md5 keys are not found or are invalid.
SYSLG8.74.68	Warning	AAA	Packet RX on interface %(1)s from %(2)s - last authentication key has expired	Key IDs do not match; keys are expired or some other key configuration problems.
SYSLG8.75.0	Warning	Web	HTTPS server has been enabled but a certificate was not found.@For certificate generation use the - @ 'crypto certificate [1-2] generate' command.@The service will start automatically	HTTPS server has been enabled but a certificate was not found. For a certificate generation use the - 'crypto certificate [1-2] generate' command. The service will start automatically when a

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			when a certificate is generated.	certificate is generated.
SYSLG8.75.66	Warning		%(2)s service has been enabled but an encryption key (certificate %(1)d) was not found.@For key generation use the 'crypto key generate' commands. The service will start automatically when a host key is generated.	The specified service has been enabled but an encryption key was not found. For key generation use the 'crypto key generate' commands. The service starts automatically when a host key is generated.
SYSLG8.77.26	Warning	AAA	Invalid attribute %(1)d ignored - %(2)s	The specified attribute is ignored.
SYSLG8.78.14	Warning	AAA	Msg of %(1)u length received from server %(3)s is bigger than maximum - %(2)u. Information is truncated.	The message length is bigger than the specified maximum. Extra characters will be truncated.
SYSLG8.78.15	Warning	AAA	Parsing of the %(1)s msg received from TACACS server %(2)s failed	Parsing of the specified message received from the specified TACACS server has failed.
SYSLG8.78.18	Warning	IP	Unexpected TCP msg was received from server %(1)s	Unexpected TCP message was received from the specified server.
SYSLG8.78.2	Warning	AAA	No TACACS+ server is configured, cannot start authentication	No TACACS+ server is configured, so authentication cannot be performed.
SYSLG8.78.23	Warning	AAA	Connection to server %(1)s is aborted. Single Connection mode may not be supported by this server.	A connection attempt to a specified server is terminated. Single connection mode is not supported by the current server.
SYSLG8.78.6	Warning	AAA	No TACACS+ server is configured, cannot start authorization	No TACACS+ server is configured, so authorization cannot be started.
SYSLG8.78.7	Warning	AAA	Cannot create new user, too many users	Cannot create new user due to too many users already configured.
SYSLG8.79.4	Warning	Up/Download	FLMNGG_update_file_state: The entry of file %(1)s was not updated to the flash	The entry to the specified file was not updated to the flash.
SYSLG8.80.2	Warning	SNMP	PIMGLG_snmp_bindmib variable: For variable id %(1)lu the snmp operation %(2)s not supported.	For the specified variable ID the SNMP operation is not supported.
SYSLG8.81.12	Warning		Func=%(1)s:Line=%(2)d: %(3)s	

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
SYSLG8.81.14	Warning		Func=%(1)s:Line=%(2)d: Unknown return value %(3)d	
SYSLG8.81.18	Warning		Func=%(2)s:Line=%(1)d: Can't allocate buffer	
SYSLG8.81.19	Warning		Func=%(2)s:Line=%(1)d: No outgoing interface	
SYSLG8.81.20	Warning		%(1)s state mashine:State:%(2)s,Event:%(3)s:GroupIp=%(4)s,SrcIp=%(5)s received	
SYSLG8.81.21	Warning		%(1)s state mashine:Incompatible State:%(2)s,Event:%(3)s for GroupIp=%(4)s,SrcIp=%(5)s received	
SYSLG8.81.6	Warning	System	Module %(1)s: Call function %(2)s without init	In the specified module the specified call function is without initialization.
SYSLG8.81.7	Warning		%(1)s: Bad state in state machine %(2)s	The specified state is not correct is the specified state machine.
SYSLG8.81.8	Warning		%(1)s: Hash table %(2)s is full	The specified hash table is full.
SYSLG8.86.0	Warning	Up/Download	Configuration update of unit %(1)lu failed. Reason: %(2)s.	The specified unit configuration update failed.
SYSLG8.86.4	Warning	SNMP	Access attempted by unauthorized NMS	Access attempted by an unauthorized NMS.
SYSLG8.86.9	Warning	Up/Download	Error encountered while downloading config: %(1)s	An error occurred while downloading the specified configuration.
SYSLG8.89.8	Warning	SNMP	Overflow in CDB	There is an overflow in CDB.
SYSLG8.89.9	Warning	SNMP	Overflow in startup CDB. offset = %(1)lu, file end = %(2)lu	
SYSLG8.9.11	Warning	FDB	Timer allocation failed	The v1 Host Timer cannot be activated, and a router will stay in the v1 state.
SYSLG8.9.14	Warning	FDB	Querier->NonQueirier transition on Interface: %(1)j	An interface stopped to be a Querier.
SYSLG8.9.7	Warning	FDB	IGMP Cache table is overflowed	No entry can be inserted - the platform reached its limit.
SYSLG8.9.8	Warning	FDB	Received IGMP wrong version (V1) query	Received a wrong IGMP version (v1) query.
SYSLG8.9.9	Warning	FDB	Received IGMP wrong	Received a wrong IGMP

ID	SEVERITY	CATEGORY	MESSAGE	DESCRIPTION
			version (V2) query	version (v2) query
SYSLG8.95.0	Warning	Up/Download	Configuration upload has been aborted	Configuration file upload has been aborted.
SYSLG8.95.1	Warning	Up/Download	Configuration download has been aborted	Configuration file download has been aborted.
SYSLG8.95.6	Warning		%(1)s	
SYSLG8.96.7	Warning		Unknown certificate subject field	
SYSLG8.98.6	Warning	System	Bad OS status	Bad OS status.
SYSLG8.98.7	Warning	FDB	Reached Maximum number of IGMP memberships	The IGMP database is full. No entry can be inserted.

C

PASSWORD RECOVERY PROCEDURE

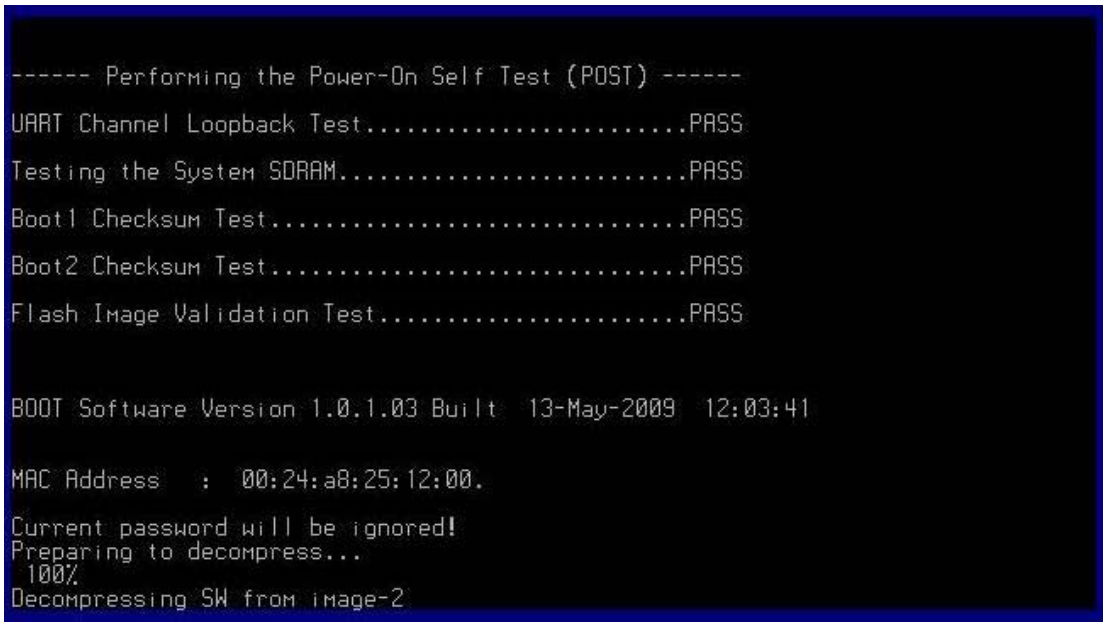
This document describes the procedure for resetting passwords on D-Link Switches.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This document will explain how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

4. **For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.**
5. **Power on the switch. After the boot image is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey (Shift + 6) to enter the "Password Recovery Mode". Once the Switch enters the "Password Recovery Mode", all ports on the Switch will be disabled.**


------ Performing the Power-On Self Test (POST) ------
UART Channel Loopback Test.....PASS
Testing the System SDRAM.....PASS
Boot1 Checksum Test.....PASS
Boot2 Checksum Test.....PASS
Flash Image Validation Test.....PASS
BOOT Software Version 1.0.1.03 Built 13-May-2009 12:03:41
MAC Address : 00:24:a8:25:12:00.
Current password will be ignored!
Preparing to decompress...
100%
Decompressing SW from image-2

6. **In the "Password Recovery Mode" only the following commands can be used.**

Command	Description
reset config	The reset config command resets the whole configuration back to the default values, with the exception of the account settings.
reboot	The reboot command exits the Password Recovery Mode and restarts the switch.
reset account	The reset account command deletes all of the created user accounts.
reset password <username>	The reset password command resets the password of the specified user. If a username is not specified, the password of all the users will be reset.
show account	The show account command displays all previously created accounts.